Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2015–2016

34 413 Wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten)

Nr. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 28 april 2016

Hoofdstuk I. Algemeen

Met belangstelling heb ik kennis genomen van de vragen van de leden van de fracties van de VVD, de PvdA, de SP, het CDA en de PVV over het bovengenoemde wetsvoorstel in het verslag. Graag ga ik op deze vragen in. Ik hoop dat de beantwoording zal bijdragen aan een voorspoedige verdere behandeling van dit wetsvoorstel. Deze nota naar aanleiding van het verslag doe ik u mede namens de Ministers van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties toekomen.

I. ALGEMEEN

1. Inleiding

De leden van de PvdA-fractie vroegen hoe de rechtstreekse werking van de verordening zich verhoudt tot de toch 19 bladzijden aan wettekst om de Nederlandse wet aan te passen. De omvang van het wetsvoorstel is te herleiden tot een optelsom van voorgestelde wijzigingen die nodig zijn voor een volledige en juiste uitvoering van de verordening met inachtneming van de rechtstreekse werking daarvan. De huidige wet bevat enkele voorschriften die met de verordening overlappen of daarmee in strijd zijn, waardoor die in het wetsvoorstel vervallen of zijn aangepast. De verordening schrijft lidstaten soms uitdrukkelijk voor nationale voorschriften vast te stellen, zoals inzake sancties die van toepassing zijn op inbreuken op de verordening waarin het wetsvoorstel vervolgens voorziet. Soms veronderstelt de verordening dat bepaalde zaken overeenkomstig nationale wetgeving plaatsvinden, zoals ten aanzien van de wijze van identificatie voorafgaand aan de afgifte van gekwalificeerde certificaten. Het wetsvoorstel bevat hierover uitgebreide voorschriften. Ook bevat de verordening verplichtingen waarvan het karakter nationale wetgeving noodzakelijk maakt ter uitvoering daarvan. De verordening verplicht bijvoorbeeld toezichthoudende organen tot het onder

kst-34413-6
ISSN 0921 - 7371
’s-Gravenhage 2016

voorwaarden verlenen van bijstand. Om bijstand te kunnen verlenen dient het toezichthoudend orgaan over daarvoor benodigde passende bevoegdheden te beschikken die de verordening zelf niet regelt en waarin het wetsvoorstel vervolgens voorziet. Ook vereist de directe werking soms inpassing in het bestuursrecht omwille van uitvoerbaarheid en rechtszekerheid. Daarnaast houdt het wetsvoorstel bijvoorbeeld rekening met de mogelijkheid dat bepaalde uitvoeringshandelingen van de Europese Commissie kunnen uitblijven, waarin dan als dat nodig is voor een goede uitvoering van de verordening (tijdelijk) nationaal kan worden voorzien. Er zijn ook andere redenen die aanpassing van wetgeving ter uitvoering van de verordening noodzakelijk maken. Er zijn bijvoorbeeld voorgestelde wijzigingen welke voorzien in de technische overgang van zaken onder toezicht van de Autoriteit Consument en Markt (hierna ook: ACM) naar Agentschap Telecom (hierna ook: AT), in vervanging van bestaande definities in diverse wetten door te verwijzen naar definities die in de verordening wordt gebruikt, in technische bepalingen die louter de samenloop met andere lopende wetsvoorstellen regelen, en in inwerkingtreding en ondertekening (blz. 12 tot en met 19; artikelen IV, VI tot en met IX, XI tot en met XV). Een optelsom van dit soort zaken leidt tot het wetsvoorstel van deze omvang.

De leden van de PvdA-fractie uitten hun zorgen over de overzichtelijkheid en inzichtelijkheid van de wetgeving voor ondernemers en consumenten. De leden vragen op welke wijze de regering dit probleem gaat ondervangen en of en op welke websites inzichtelijk wordt gemaakt hoe de nieuwe wet- en regelgeving rondom elektronische identiteiten en vertrouwensdiensten eruit komt te zien. De samenhangende wetgeving dient overzichtelijk en inzichtelijk voor ondernemers en consumenten te zijn. Om dit te bewerkstelligen zal er op de website van het Ministerie van Economische Zaken een tabel worden geplaatst met in de eerste kolom alle artikelen van de verordening. In de volgende kolommen wordt zichtbaar gemaakt of het betreffende artikel nadere uitwerking kent in uitvoeringshandelingen op grond van de verordening dan wel dit wetsvoorstel of de daarop te baseren algemene maatregel van bestuur. Daarbij kan bij meer omvangrijke teksten of toelichting gebruik worden gemaakt van hyperlinks naar de oorspronkelijke teksten. Op deze wijze is in een oogopslag duidelijk wat de regels zijn en op welke wijze deze met elkaar samenhangen.

De leden van de PvdA-fractie vroegen zich af waarom de meerdere algemene maatregelen van bestuur uit het wetsvoorstel niet worden voorgehangen bij de Tweede Kamer. Er is niet voorzien in een voorhangprocedure omdat de onderwerpen waarvoor een algemene maatregel van bestuur kan worden vastgesteld een meer technische uitwerking van het wetsvoorstel zijn. Dit geldt temeer nu het om tenuitvoerlegging van Europese regelgeving gaat. De Aanwijzingen voor de regelgeving (Ar 35) zijn gevolgd met daarin het uitgangspunt dat bij gedelegeerde regelgeving geen voorhang wordt geregeld. De algemene maatregel van bestuur als bedoeld in het voorgestelde artikel 18.15 van de Telecommunicatiewet (onderdeel P) heeft betrekking op het aanwijzen van technische referentienormen waaraan een vermoeden van overeenstemming met daarop betrekking hebbende eisen uit de verordening kan worden ontleend. Op dit moment is er niet een concreet voornemen dergelijke referentienormen bij of krachtens algemene maatregel van bestuur aan te wijzen. De in het voorgestelde artikel 18.15a van de Telecommunicatiewet (onderdeel Q) bedoelde algemene maatregel van bestuur beperkt zich tot het stellen van regels over de te verstrekken gegevens en de wijze van verstrekking bij een inbreuk op de veiligheid of verlies van integriteit aan de in het wetsvoorstel aangewezen organen en aan degene aan wie een vertrouwensdienst is verleend die naar verwachting ongunstige gevolgen

zal ondervinden van de inbreuk. Hierover zijn door de Europese Commissie vooralsnog geen uitvoeringshandelingen vastgesteld, zodat het voornemen is hier bij algemene maatregel van bestuur in te voorzien. Een eventuele algemene maatregel van bestuur als bedoeld in het voorgestelde artikel 18.17a, zevende lid (onderdeel T) beperkt zich tot aan de Minister te verstrekken gegevens en de wijze van verstrekking daarvan door een instelling die wenst te worden aangewezen als certificerende instelling voor gekwalificeerde middelen. Het voornemen is om met betrekking tot de in artikel 18.15a en 18.17a genoemde onderwerpen in één enkele algemene maatregel van bestuur nadere regels te stellen.

De leden van de CDA-fractie wilden weten of de voorstellen zijn getoetst aan de hand van het subsidiariteitsbeginsel en zo ja of er artikelen zijn die volgens de regering beter nationaal geregeld zouden kunnen worden. De verordening beoogt de wederzijdse erkenning en aanvaarding van elektronische identiteiten en vertrouwensdiensten in andere lidstaten te vereenvoudigen. Hiervoor is wetgeving op Europees niveau gepast en wenselijk. Met op zichzelf staande nationale wetgeving kan dit doel niet worden bereikt. Zonder een verordening komt de wederzijdse erkenning van nationaal uitgegeven elektronische identificatiemiddelen, elektronische handtekeningen, en overige vertrouwensdiensten op de Europese markt moeilijk van de grond en blijven deze veelal slechts bruikbaar binnen de landsgrenzen. De verordening is een resultaat van de besluitvorming waaraan alle lidstaten van de Europese Unie hebben deelgenomen. De verordening heeft rechtstreekse werking en is bindend voor alle lidstaten van de Europese Unie. Nationale voorschriften zijn mogelijk voor zover de verordening hiertoe verplicht of ruimte laat. Het wetsvoorstel voorziet daarin voor zover dit voor een goede uitvoering van de verordening vereist is.

De leden van de CDA-fractie stelden de vraag of de regering bij de omzetting van Europese regelgeving alleen datgene heeft omgezet wat strikt genomen op grond daarvan noodzakelijk is. Het wetsvoorstel strekt uitsluitend tot omzetting van de verordening. Het uitgangspunt van de rechtstreekse werking van de verordening en minimumomzetting wordt door middel van het wetsvoorstel gerespecteerd. Bij de uitwerking is telkens bezien welke in het wetsvoorstel op te nemen voorschriften voor een goede uitvoering van de verordening vereist zijn. In de artikelsgewijze toelichting is op de daarbij gemaakte afwegingen op specifieke onderdelen nader ingegaan.

De leden van de CDA-fractie vroegen of het wetsvoorstel eraan bijdraagt dat Nederlandse bedrijven internationaal met aanbestedingen mee kunnen doen en of het wetsvoorstel bijdraagt aan de vereenvoudiging van vergunningen in andere lidstaten.
In de huidige situatie hebben aanbestedende diensten die een elektronische inschrijving toestaan de mogelijkheid een geavanceerde elektronische handtekening te eisen. De herziene aanbestedingsrichtlijnen, te weten richtlijn 2014/24/EU van het Europees parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PbEU 2014, L 94) en richtlijn 2014/25/EU van het Europees parlement en de Raad van 26 februari 2014 betreffende het plaatsen van opdrachten in de sectoren water- en energievoorziening, vervoer en postdiensten en houdende intrekking van Richtlijn 2004/17/EG (PbEU 2014, L 94), bevatten voor aanbestedende diensten en speciale-sectorbedrijven verplichtingen inzake elektronisch aanbesteden en bevatten daarbij ook voorschriften over de erkenning van geavanceerde elektronische handtekeningen die voldoen aan bepaalde formats. Dit vergemakkelijkt voor het Nederlandse bedrijfsleven straks het op afstand en grensoverschrijdend mee kunnen doen aan aanbestedingen

doordat elektronisch aanbesteden de regel wordt en zij daarbij voor ondertekening van documenten bepaalde elektronische handtekeningen kunnen gebruiken die lidstaten moeten accepteren. Door de verordening wordt het bovendien mogelijk om andere vertrouwensdiensten, zoals een elektronisch tijdstempel of dienst voor aangetekende elektronische bezorging bij aanbestedingen of het aanvragen van vergunningen in andere lidstaten te gebruiken. De inhoud van het verkeer blijft hetzelfde maar door het gebruik van vertrouwensdiensten wordt de betrouwbaarheid en de rechtszekerheid bij digitale communicatie verhoogd. De verordening helpt daarbij doordat Nederlandse bedrijven hun eigen elektronische handtekening, -tijdstempel, -zegel of dienst voor aangetekende elektronische bezorging kunnen gebruiken voor procedures, vergunningen en transacties in andere lidstaten.

De leden van de CDA-fractie wilden weten wat Nederland wel en niet heeft binnengehaald bij de onderhandelingen over de verordening ten aanzien van de punten uitvoerbaarheid, veiligheid, effectief toezicht en daarbij de aansprakelijkheid van de staat. De leden vragen waarom het voorstel uitvoerbaar is.
Mede dankzij de Nederlandse inzet is het toezicht op de vertrouwensdienstverlening uitgebreid en op onderdelen sterk verbeterd. Zo vallen de zogenoemde certificaten voor de authenticatie van websites binnen de verordening waardoor toezicht mogelijk wordt. Deze certificaten worden veel gebruikt en garanderen dat de bezoeker zich op de echte site van een webwinkel, overheidsorganisatie of internetbankomgeving bevindt en niet op een namaaksite. Daarnaast is het voorafgaande toezicht op de zogeheten gekwalificeerde vertrouwensdiensten versterkt. De toezichthouder moet vaststellen dat deze diensten aan de wettelijke eisen voldoen alvorens deze aan het publiek mogen worden aangeboden. Verder richten de conformiteitsbeoordelingen en het toezicht zich meer op de verleende vertrouwensdiensten zelf en minder op het managementsysteem van de aanbieder(s). Ook biedt de verordening mogelijkheid tot samenwerking tussen toezichthouders bij incidenten met grensoverschrijdende impact. Voor niet-gekwalificeerde vertrouwensdiensten geldt een licht toezichtregime. Dit betekent dat de aanbieders van deze diensten incidenten met aanzienlijke gevolgen moeten melden bij de toezichthouder die vervolgens een onderzoek kan instellen. Deze vorm van toezicht is een compromis waarbij het belang van veiligheid is afgewogen tegen de administratieve lasten die met toezicht gepaard gaan. De veiligheid is ermee gebaat dat alleen elektronische identificatiemiddelen van een substantieel en hoog niveau grensoverschrijdend geaccepteerd moeten worden. In geval van veiligheidsincidenten moet dit worden gemeld bij de Europese Commissie en is verplichte acceptatie (tijdelijk) niet aan de orde. De verordening maakt het mogelijk dat private partijen elektronische identiteiten aanbieden die grensoverschrijdend kunnen worden erkend, zonder dat de aansprakelijkheid hiervoor door de staat wordt overgenomen.
De verordening is uitvoerbaar omdat er inmiddels nationaal ruime ervaring is opgedaan met elektronische handtekeningen en andere vertrouwensdiensten, zoals de certificaten voor de authenticatie van websites. Hoewel de inrichting van een internetpagina of formulier in een andere lidstaat er anders dan gewend uit kan zien, verloopt het inloggen of ondertekenen op de voor de burger of het bedrijf vertrouwde manier. Om de grensoverschrijdende erkenning van elektronische identiteiten door openbare instanties mogelijk te maken, wordt verder gewerkt aan het elektronisch knooppunt (hierna verder: eIDAS-knooppunt). Uit proefprojecten blijkt dat dit knooppunt werkt. Dit dient de uitvoerbaarheid van het voorstel. Net als richtlijn 1999/93/EG van het Europees parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG 2000, L 13) (hierna: de

Richtlijn of Richtlijn elektronische handtekeningen) maakt de verordening onderscheid in gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten. De ervaring met de Richtlijn heeft geleerd dat dit onderscheid in de praktijk soms moeilijk te vatten is. In Nederland heeft het Forum Standaardisatie een handreiking ontwikkeld om proceseigenaren te helpen de juiste elektronische identiteit of vertrouwensdienst bij hun dienst te kiezen.

De leden van de CDA-fractie informeerden naar de gevolgen van het wetsvoorstel voor inwoners die het lastig vinden om mee te komen met de digitale wereld, en zo ja wat die gevolgen zijn en welke alternatieven er voor hen zijn. Voor deze inwoners zijn aan de verordening en het wetsvoorstel geen gevolgen verbonden. Doel van de verordening is het vertrouwen in elektronische transacties te vergroten met behulp van elektronische identificatiemiddelen en vertrouwensdiensten. Geen onderwerp van de verordening en het wetsvoorstel is bijvoorbeeld het verplichten van burgers om gebruik te maken van elektronische identificatiemiddelen of van vertrouwensdiensten. Het wetsvoorstel beperkt de keuzevrijheid van burgers derhalve niet.

Naar aanleiding van de vraag van de leden van de CDA-fractie waarom het wetsvoorstel geen evaluatiebepaling bevatte en bij de algemene maatregelen van bestuur geen voor- en/of nahangbepalingen waren opgenomen, merk ik het volgende op. Het wetsvoorstel strekt uitsluitend tot uitvoering van de verordening die voor alle lidstaten van de Europese Unie met rechtstreekse werking van toepassing is. Gelet hierop is er voor gekozen in het wetsvoorstel geen evaluatiebepaling op te nemen. Dit laat onverlet dat de verordening zelf een evaluatiebepaling over de toepassing van de verordening kent, met name op enkele specifieke onderdelen daarvan (artikel 49). Uiterlijk op 1 juli 2020 dient door de Europese Commissie over die toepassing verslag te worden uitgebracht bij het Europees parlement en de Raad van de Europese Unie, in voorkomend geval vergezeld van wetgevingsvoorstellen. Voor een reactie op de vraag over de voor- en/of nahangbepalingen verwijs ik deze leden naar het antwoord in deze paragraaf op een vergelijkbare vraag van de leden van de PvdA-fractie.

De leden van de PVV-fractie vroegen naar de betrouwbaarheid van buitenlandse elektronische identiteiten en vertrouwensdiensten en waarop dit vertrouwen gebaseerd is. Het vertrouwen in buitenlandse elektronische identiteiten is gebaseerd op de eisen uit de verordening voor betrouwbaarheid van elektronische identificatiemiddelen uit andere lidstaten en de procedure voor aanmelding bij de Europese Commissie. De verordening definieert de betrouwbaarheidsniveaus «laag», «substantieel» en «hoog». Deze indeling in betrouwbaarheidsniveaus houdt rekening met de internationale norm ISO/IEC 29115, de belangrijkste internationale norm op het gebied van betrouwbaarheidsniveaus voor elektronische identificatiemiddelen. De specificaties voor betrouwbaarheidsniveaus bevatten eisen aan het controleren van de identiteit van de verzoeker waardoor een elektronisch identificatiemiddel niet zomaar aan een ander persoon kan worden uitgegeven. Nadat een lidstaat een stelsel met één of meer middelen aanmeldt en het notificatieproces hiervoor volledig heeft doorlopen moet Nederland op basis daarvan middelen van «substantieel» of «hoog» niveau uit die lidstaten accepteren. Concreet maakt het niveau «substantieel» gebruik van ten minste twee authenticatiefactoren. Bij dat niveau wordt de identiteit bijvoorbeeld aangetoond aan de hand van een bewijsstuk (zoals registers of nationaal erkende documenten) dat wordt erkend door die lidstaat. Voor de uitgifte is afgesproken dat het elektronische identificatiemiddel wordt uitgereikt op zo'n wijze dat verondersteld mag worden dat alleen de persoon aan wie

het toebehoort in het bezit ervan wordt gesteld. Voor hoog gelden nog strengere eisen. Uitvoeringsverordening 2015/1502 van de Europese Commissie tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 (PbEU 2015, L 235/7) (hierna verder: Uitvoeringsverordening betrouwbaarheidsniveaus) beschrijft verder in detail de minimale technische specificaties en procedures van de betrouwbaarheidsniveaus. De lidstaten moeten er zelf voor zorgen dat hun elektronische identificatiemiddelen aan de bij of krachtens de verordening gestelde eisen voldoen. Uitvoeringsverordening 2015/1984 van de Europese Commissie van 3 november 2015 tot vaststelling van de omstandigheden, formaten en procedures voor aanmeldingen in het kader van artikel 9, lid 5, van Verordening (EU) nr. 910/2014 (PbEU 2015, L 289/18) (hierna: Uitvoeringsverordening aanmeldingsprocedure) beschrijft de informatie die lidstaten moeten aanleveren aan de Europese Commissie. Voordat lidstaten hun stelsels van elektronische identificatiemiddelen kunnen aanmelden bij de Europese Commissie, zullen lidstaten samenwerken om de stelsels voor elektronische identificatie die onder deze verordening vallen onderling te evalueren. Het aanmeldingsformulier verwijst onder andere naar de uitkomsten van deze evaluatie en eventuele externe audits. Op deze manier dienen de elektronische identificatiemiddelen van andere lidstaten aan de afgesproken vereisten op Europees niveau te voldoen. Voor vertrouwensdiensten geldt dat deze onder toezicht vallen van de nationale toezichthouders. Voor de zogeheten gekwalificeerde vertrouwensdiensten geldt dat de toezichthouder controleert of aan de eisen van de verordening is voldaan voordat deze diensten aangeboden worden aan het publiek. Voor niet-gekwalificeerde vertrouwensdiensten geldt een lichter toezichtregime waarbij de toezichthouder de mogelijkheid heeft om naar aanleiding van een melding of incident onderzoek te verrichten. In antwoord op eerdere vragen van de leden van de CDA-fractie in paragraaf 1 over wat Nederland bij de onderhandelingen over de verordening heeft binnengehaald, is deze systematiek uiteengezet.

De leden van de PVV-fractie vroegen waarom blindelings vertrouwd moet worden op elektronische identificatiemiddelen van andere lidstaten, mede in het licht van het in opspraak zijn van DigiD in het verleden. In het antwoord op de vorige vraag van deze leden is reeds ingegaan op de basis van het vertrouwen in identificatiemiddelen van andere lidstaten. De aanmeldende lidstaat moet zich vergewissen dat het aan te melden middel aan het normenkader voor betrouwbaarheidsniveaus voldoet. Tijdens de onderlinge evaluatie, die onderdeel is van de aanmeldingsprocedure bij de Commissie, kunnen andere lidstaten het middel daarop toetsen. Mochten zich toch veiligheidsproblemen voordoen met middelen van andere lidstaten, dan is op Europees niveau afgesproken dat lidstaten elkaar en de Europese Commissie moeten informeren. Artikel 10 van de verordening bepaalt dat een door een veiligheidsinbreuk of integriteitsverlies getroffen lidstaat de grensoverschrijdende authenticatie geheel of gedeeltelijk moet opschorten of intrekken.

De leden van de PVV-fractie wilden weten of Nederland als lidstaat niet zelf kan bepalen welk elektronisch identificatiemiddel betrouwbaar is en welke middelen niet. De verordening laat Nederland geen ruimte om zelf in andere lidstaten onderzoek te doen en te bepalen of een elektronisch identificatiemiddel van een andere lidstaat aan de gestelde eisen voldoet. De verordening heeft als doel om grensoverschrijdend gebruik van onlinediensten bij openbare instanties in Europa te vergemakkelijken. De verordening stelt een aantal voorwaarden om erkenning mogelijk te maken.

Het proces dat tot verplichte erkenning leidt, laat geen beoordeling door individuele lidstaten toe. Bovendien zou het stuk voor stuk beoordelen van elektronische identiteiten van de andere lidstaten leiden tot een groot aantal onderlinge toetsingen en daarmee gepaard gaande lasten. Deze belasting zou zowel voor Nederland zelf, als voor de overige lidstaten gelden. Samenwerking bij toetsing is efficiënter.

De leden van de PVV-fractie informeerden naar de implicaties van het wetsvoorstel op fraude bij overheidsdiensten, zoals ook met DigiD is gebeurd. Deze leden wilden weten of dit voorstel de deur openzet voor misbruik van de nationale sociale voorzieningen. De verordening maakt het mogelijk dat burgers hun elektronische identificatie kunnen gebruiken om zich elektronisch kenbaar te maken in een andere lidstaat. Voor overheidsdienstverleners betekent dit dat zij de persoonsidentiteitsgegevens met een substantieel of hoog niveau van betrouwbaarheid krijgen aangeleverd. Het authentiseren van een gebruiker is (net als met DigiD) echter iets anders dan het toekennen van rechten, zoals sociale voorzieningen. Met behulp van een geslaagde authenticatie kan een aanvraag worden gedaan. Deze wordt beoordeeld op juistheid, volledigheid en rechtmatigheid. Op basis hiervan wordt een beslissing genomen over het al dan niet toekennen van rechten. De uitvoeringsdiensten, gemeenten, provincies en waterschappen blijven, net als nu verantwoordelijk voor de inrichting van hun werkprocessen en de rechtmatigheidsbeoordeling voor afname van hun dienst(en), met inbegrip van de nationale sociale voorzieningen.

De leden van de PVV-fractie wilden graag een overzicht van de publieke diensten ontvangen waar de verplichte erkenning van elektronische identificatiemiddelen van toepassing wordt. De verordening regelt dat wanneer een nationale overheidsdienst al online toegankelijk is met een nationaal erkend elektronisch identificatiemiddel, gebruikers met een bij de Europese Commissie aangemeld middel uitgegeven in een andere lidstaat ook erkend zouden moeten worden. De overheidsdiensten die toegankelijk zijn met DigiD zijn hier te vinden: https://www.digid.nl/over-digid/wie-doen-mee/. De overheidsdiensten die toegankelijk zijn met eHerkenning zijn hier te vinden: https://www.eherkenning.nl/aansluiten-op-eherkenning/wie-zijn-aangesloten/. Op de beide genoemde websites staan ook private partijen genoemd, die buiten de plicht vallen om identificatiemiddelen uit andere lidstaten te erkennen.

De leden van de PVV-fractie wilden weten of Nederlandse elektronische identificatiemiddelen ook in het buitenland gebruikt kunnen worden, bijvoorbeeld bij een Poolse webwinkel. Op grond van de verordening krijgen Nederlandse burgers een mogelijkheid om met een middel op niveau «substantieel» of «hoog» elektronisch zaken te doen met openbare instanties in andere lidstaten op basis van de wederzijdse erkenning van elkaars middelen. Private Poolse webwinkels bepalen zelf of ze elektronische identificatiemiddelen uit andere lidstaten accepteren. Voor private partijen is deze acceptatie niet verplicht. Als private partijen ervoor kiezen om elektronische identificatiemiddelen uit andere landen te accepteren die bij de Europese Commissie zijn aangemeld, moeten ze wel aansluiten op een voorziening voor onlineauthenticatie. Authenticatie is de bevestiging van een beweerde identiteit. Hier is in Nederland het zogenoemde eIDAS-knooppunt voor ontwikkeld (hierna verder te noemen: het eIDAS-knooppunt). Nederland kan zijn nationale stelsel(s) voor elektronische identificatie – welke wettelijk wordt(en) ingekaderd -bij de Europese Commissie aanmelden. Na het doorlopen van de aanmeldingsprocedure en de publicatie op een lijst door de Europese Commissie moeten alle lidstaten die elektronische identificatiemiddelen uit een aangemeld stelsel van de desbetreffende lidstaat accepteren. Er is nog

geen besluit genomen of en, zo ja, wanneer een of meer nationale stelsels, met daarbinnen de middelen, worden aangemeld. Een vereiste is dat een nationaae stelsel voor elektronische identificatiemiddelen eerst moet voldoen aan alle eisen die de verordening stelt. Zo zal de indeling in betrouwbaarheidsniveaus van de inlogmiddelen moeten aansluiten op de normen uit de verordening.

De leden van de VVD-fractie vroegen zich af in hoeverre bij het gebruik van persoonsidentificatiegegevens nadere eisen worden gesteld aan het inrichten van de beheerprocessen binnen een ICT-organisatie, zoals die benodigd zijn voor het opstellen en uitgeven van elektronische identiteiten en vertrouwensdiensten. Bij het gebruik van elektronische identiteiten moeten persoonsidentificatiegegevens een aantal punten passeren om van een gebruiker in lidstaat A naar de overheidsorganisatie in lidstaat B te gaan. Deze punten moeten voldoen aan nationale en Europese eisen aan beheersprocessen binnen een ICT-organisatie (ISO standaarden voor informatiebeveiliging en service managementsystemen -ISO27000-serie). Op deze manier weten openbare instanties in land A dat in land B aan de minimale vereisten is voldaan. In de eerder genoemde Uitvoeringsverordening betrouwbaarheidsniveaus zijn deze minimale vereisten aan zowel het beheer van de (uitgever van) identificatiemiddelen, als het beheer van informatiebeveiliging door de overheidsdienstverlener opgenomen, te weten ISO/IEC 27000 en de ISO/IEC 20000 series. Nederlandse partijen, zowel de beheerder van het eIDAS-knooppunt (het Ministerie van Economische Zaken), als de deelnemers aan een door Nederland aangemeld nationaal stelsel voor elektronische identificatie zullen moeten voldoen aan de ISO/IEC 27001 normen voor informatiebeveiliging. ISO 27001 biedt een model voor het vaststellen, implementeren, bijhouden en continu verbeteren van een zorgsysteem voor informatiebeveiliging, ook wel een «Information Security Management System» (ISMS) genoemd. Het ISMS beschermt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie door een risicobeheerproces toe te passen. Overheidspartijen houden zich bovendien aan de Baseline Informatiebeveiliging rijksoverheid (BIR). Voor vertrouwensdiensten geldt dat deze moeten voldoen aan in de verordening bepaalde eisen. Door internationale standaardisatieorganisaties opgestelde standaarden, geven nadere invulling aan de beheerprocessen van vertrouwensdienstverleners.

De leden van de VVD-fractie vroegen naar de kaders voor het inrichten van beheerprocessen, zoals Information Technology Infrastructure Library (ITIL). De beheerprocessen van het eIDAS-knooppunt door het Ministerie van Economische Zaken zijn gebaseerd op ITIL (gericht op systeembeheer) en ASL («Application Services Library»). ASL richt zich op de processen van het beheer, onderhoud en vernieuwing van informatiesystemen en applicaties zoals het eIDAS-knooppunt. Onderdeel van de jaarlijkse ISO 27001 certificering is beoordeling van de werking van de beheerprocessen.

2. De eidas-verordening en gerechtvaardigd vertrouwen in digitaal verkeer

2.1 Elektronische identificatie en elektronische identificatiemiddelen

2.2 Vertrouwensdiensten

De leden van de CDA-fractie vroegen zich af in hoeverre de in het wetsvoorstel genoemde vertrouwensdiensten nog kinderziektes bevatten en of het gebruik van vertrouwensdiensten volledig veilig is. De verordening maakt onderscheid in gekwalificeerde en niet gekwalificeerde vertrouwensdiensten. De zogeheten gekwalificeerde vertrouwensdiensten

moeten voldoen aan in de verordening gestelde eisen. Deze vertrouwensdiensten zijn gebaseerd op cryptografische technieken, die zelf inmiddels het stadium van kinderziektes voorbij zijn. Er is echter altijd een afweging tussen veiligheid enerzijds en gebruiksgemak en kosten anderzijds. Een nieuwe ontwikkeling waar in de verordening ruimte voor is gemaakt, is die van ondertekenen op afstand. Daarbij is het sleutelmateriaal zelf niet in bezit van de ondertekenaar. Deze nieuwe ontwikkeling is op het gebied van de technische standaarden nog niet volledig uitgekristalliseerd. Gekwalificeerde vertrouwensdiensten kennen strengere technische (beveiligings)eisen dan niet-gekwalificeerde diensten, de gebruiksvriendelijkheid is daardoor echter soms minder. Niet-gekwalificeerde vertrouwensdiensten zijn in principe ook veilig, afhankelijk van waar ze voor worden gebruikt, maar de waarborgen zijn minder. Voor sommige doeleinden vinden gebruikers dit acceptabel. De acceptatie van vertrouwensdiensten is gebaat bij gebruikersvriendelijkheid én veiligheid. Daarbij hebben gebruikers van vertrouwensdiensten ook een verantwoordelijkheid voor veilig gebruik van vertrouwensdiensten. Bijvoorbeeld door de eigen ICT-omgeving te beveiligen en zich te houden aan de gebruiksvoorschriften van de vertrouwensdienstverlener. Zoals bekend, bestaat 100% veiligheid niet. De kans op een veiligheidsinbreuk wordt echter aanzienlijk gereduceerd als zowel de vertrouwensdienstverlener als de gebruikers de wettelijke- en gebruiksvoorschriften naleven.

2.3 Certificaten onderdeel van vertrouwensdiensten

De leden van de D66-fractie vroegen of verificatie van de identiteit in fysieke aanwezigheid ook onder de huidige regelgeving het geval is, en zo niet of er dan wel sprake is van een vereenvoudiging van het verkrijgen van een certificaat. Het antwoord is bevestigend. Artikel 18.15 van de Telecommunicatiewet bepaalt dat een certificatiedienstverlener, alvorens een gekwalificeerd certificaat af te geven, de identiteit van de persoon die als ondertekenaar in dat gekwalificeerde certificaat wordt aangeduid, vaststelt aan de hand van de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten. Uit de huidige wet volgt daarmee dat verificatie van de identiteit voorafgaand aan de afgifte van enig gekwalificeerd certificaat uitsluitend in fysieke aanwezigheid kan plaatsvinden. In de huidige situatie kan derhalve niet een gekwalificeerd certificaat worden afgegeven op basis van bijvoorbeeld identificatie aan de hand van een reeds eerder afgegeven en nog geldig elektronisch identificatiemiddel of een reeds eerder en nog geldig afgegeven gekwalificeerd certificaat.

De leden van de D66-fractie stelden de vraag of er geen mogelijkheid voor Nederland is om voor natuurlijke personen en rechtspersonen ook slechts via een elektronische procedure een gekwalificeerd certificaat aan te vragen. De verordening voorziet in drie mogelijkheden voor identificatie die elektronisch en op afstand kunnen worden uitgevoerd voorafgaand aan de afgifte van een gekwalificeerd certificaat. Voor twee van die mogelijkheden biedt de verordening de keuze aan de dienstverlener welke hij daarvan wil gebruiken. Of een vertrouwensdienstverlener ook de laatste mogelijkheid kan gebruiken, hangt af van de keuze die de lidstaat daarin maakt. De eerste mogelijkheid is dat identificatie op afstand plaatsvindt door middel van een geldig elektronisch identificatiemiddel met het betrouwbaarheidsniveau substantieel of hoog als bedoeld in de verordening, waarbij ten tijde van de uitgifte van dat middel identificatie in fysieke aanwezigheid wel heeft plaatsgevonden. De tweede mogelijkheid bestaat uit verificatie van de identiteit aan de hand van een eerder afgegeven, geldig gekwalificeerd certificaat voor de elektronische handtekening of voor het elektronische zegel. Identificatie met behulp van een dergelijk eerder afgegeven gekwalificeerd certificaat is alleen

toegestaan, indien dat eerdere certificaat ofwel in fysieke aanwezigheid is afgegeven ofwel met een elektronisch identificatiemiddel dat voldoet aan de eisen die hiervoor bij de eerste mogelijkheid zijn genoemd. Ten aanzien van deze beide mogelijkheden bepaalt het voorgestelde artikel 18.15c van de Telecommunicatiewet dat het elektronisch identificatiemiddel of het gekwalificeerd certificaat met behulp waarvan een ander gekwalificeerd certificaat online kan worden verzocht, daarvoor alleen geschikt is indien die aan de daarin in het wetsvoorstel gestelde eisen betreffende fysieke identificatie voldoen. De derde mogelijkheid voor elektronische identificatie op afstand is voor lidstaten optioneel. Lidstaten kunnen er voor kiezen andere op nationaal niveau erkende identificatiemethoden die een mate van betrouwbaarheid verschaffen die gelijkwaardig is als fysieke aanwezigheid te accepteren als alternatief voor identificatie in fysieke aanwezigheid. Anders dan bij de eerste twee mogelijkheden is bij deze derde mogelijkheid denkbaar dat een gekwalificeerd certificaat wordt afgegeven zonder dat er ooit op enig moment een eerdere, eerste fysieke identificatie heeft plaatsgevonden. Hierbij zou bijvoorbeeld wellicht kunnen worden gedacht aan beeldverbindingen, die voldoende zekerheid bieden dat een persoon daadwerkelijk live in beeld is en zijn identiteit met voldoende zekerheid aan de hand van authentieke documenten kan worden vastgesteld. De verordening stelt als voorwaarde dat het met fysieke identificatie gelijkwaardige betrouwbaarheidsniveau dan door een conformiteitsbeoordelingsinstantie bevestigd dient te zijn. Gelet op het uitgangspunt van minimumomzetting van de verordening, is in het kader van de voorbereiding van het wetsvoorstel er vanaf gezien deze mogelijkheid nader te onderzoeken.

De leden van de PVV fractie wezen op het risico dat in verschillende zuidelijke en Oost-Europese lidstaten anders wordt gedacht over de betrouwbaarheid van de eigen publieke instellingen en vroegen zich af in hoeverre het verantwoord is dat overheidsdienstverleners aldaar toegang mogen krijgen tot elektronische identificatiegegevens van Nederlandse burgers. Openbare instanties in de lidstaten moeten voldoen aan de in nationaal recht geïmplementeerde Richtlijn 95/46/EG van het Europees parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG 1995, L 281) (hierna: Richtlijn bescherming persoonsgegevens).Deze wordt vervangen door een Verordening die op Europees niveau de bescherming van persoonsgegevens regelt en die op 14 april 2016 is aangenomen door het Europees parlement. Zowel de huidige richtlijn als de nieuwe verordening voorzien in een toezichthouder per lidstaat die toezicht houdt op de bescherming van persoonsgegevens. Dit omvat ook de verwerking van persoonsidentificatiegegevens van Nederlandse burgers.

De leden van de PVV-fractie vroegen zich af in hoeverre deze verordening een verplichting wordt voor Nederlandse gebruikers die in een andere Europese lidstaat een overheidsdienst willen afnemen en of zij dat alleen elektronisch kunnen doen met een Nederlands elektronisch identificatiemiddel. De andere lidstaten of de openbare instanties uit die andere lidstaten bepalen zelf de wijze waarop zij hun dienstverlening toegankelijk maken voor eventuele Nederlandse gebruikers. Indien de dienst elektronisch toegankelijk is en daarvoor identificatie en authenticatie vereist is, op grond van nationaal recht of door gangbare bestuursrechtelijke praktijk, en Nederland zijn nationale stelsel voor elektronische identificatie heeft aangemeld kan een Nederlandse burger zijn elektronische identificatiemiddel gebruiken voor toegang tot die dienst. Het identificatiemiddel dient wel te voldoen aan het vereiste betrouwbaarheidsniveau. Een Nederlandse burger kan ook een elektronisch identificatiemiddel gebruiken dat in een andere lidstaat is uitgegeven en waarvan het

onderliggende stelsel bij de Europese Commissie is aangemeld, indien dat middel voldoet aan het vereiste betrouwbaarheidsniveau. De lidstaten of de openbare instanties afkomstig uit die lidstaten bepalen zelf of hun diensten, naast de digitale weg ook nog op andere wijze, bijvoorbeeld met papieren aanvraagformulieren kunnen worden afgenomen.

De leden van de PVV-fractie wezen op het risico dat buitenlandse, met name Oost-Europese, burgers misbruik zouden kunnen maken van Nederlandse overheidsdiensten, bijvoorbeeld door aanspraak te maken op bepaalde toeslagen en subsidies. Zij vroegen zich af of de verordening dit makkelijker maakt. In antwoord op een eerdere vraag van deze leden in paragraaf 1 over fraude bij overheidsdiensten is reeds ingegaan op mogelijk misbruik van elektronische identificatie bij overheidsdiensten. Het elektronisch aanvragen van voorzieningen, zoals subsidies en toeslagen, moet worden onderscheiden van het toekennen hiervan. De uitvoeringsdienst, gemeente of provincie blijft net als nu verantwoordelijk voor het feitelijk beoordelen van het recht op de aangevraagde dienst(en) en de toekenning daarvan op basis van algemene of sectorale wet- of regelgeving.

De fractie van de PVV vroeg op welke manier de regering met de inwerkingtreding van de eIDAS-verordening wil voorkomen dat gebruikers uit andere lidstaten steeds vaker een beroep doen op Nederlandse overheidsdiensten, met name de sociale voorzieningen. De verordening regelt de wederzijdse erkenning van elektronische identificatiemiddelen tussen lidstaten en niet de feitelijke toekenning van sociale voorzieningen. Er zal in de praktijk -net als nu het geval is- gecontroleerd moeten worden of een burger of bedrijf recht heeft op een voorziening. Vrijwel nooit zijn de persoonsidentificatiegegevens op een paspoort, zoals naam en geboortedatum, toereikend voor het toekennen van een voorziening. Een dienst heeft behoefte aan aanvullende gegevens, zoals bijvoorbeeld het aantal kinderen, recht op pensioen, een kenteken of opgebouwde rechten in het kader van een werkloosheidsuitkering. Dit type gegevens levert het eIDAS-knooppunt niet aan en deze gegevens zullen op basis van algemene of sectorale wet- of regelgeving via de huidige, gangbare praktijk verkregen moeten worden voordat een dienst wordt verleend. Op deze manier worden net als nu, de risico's van misbruik van Nederlandse overheidsdiensten ondervangen.

De leden van de PVV-fractie vroegen of de regering kan aangeven op welke manier een Nederlandse burger straks kan controleren wie er toegang heeft tot zijn of haar elektronische identificatie. Uit de Europese Richtlijn Bescherming Persoonsgegevens die in de nationale wetgeving van de lidstaten van de Europese Unie is geïmplementeerd volgt dat bij elke openbare instantie waar de elektronische identificatiemiddelen wordt gebruikt, nagevraagd kan worden wie er toegang heeft tot die gegevens en op welke wijze de persoonsidentificatiegegevens gebruikt worden.

De leden van de PVV-fractie verzochten de regering aan te geven op welke manier een Nederlandse burger de toegang tot een buitenlandse dienst eenzijdig kan intrekken, wijzigen of blokkeren. Door in te loggen stemt een gebruiker in met de verzending van de minimale set persoonsidentificatiegegevens in een andere lidstaat die nodig zijn voor identificatie en authenticatie (proces van bevestiging dat ik echt degene ben, die ik zeg dat ik ben). Weigert een gebruiker die gegevens nogmaals de grens over te sturen, dan zal de dienst verder niet elektronisch afgenomen kunnen worden.

3. De Inhoud en uitvoering van de eidas-verordening op hoofdlijnen

3.1 Inhoud eidas-verordening op hoofdlijnen

De leden van de D66-fractie vroegen toelichting bij de zinsnede «een lidstaat niet verplicht is tot het aanmelden van een stelsel bij de Europese Commissie over te gaan om erkenning te bewerkstelligen». In de overwegingen bij de verordening wordt uitdrukkelijk vermeld dat lidstaten niet verplicht dienen te worden hun stelsels voor elektronische identificatie aan de Commissie te melden. Het staat de lidstaten vrij om alle, sommige dan wel geen van de stelsels voor elektronische identificatie die op nationaal niveau worden gebruikt om ten minste toegang te krijgen tot publieke onlinediensten of specifieke diensten, aan de Commissie te melden (overweging 13 van de verordening). Het staat Nederland en andere lidstaten op grond van artikel 7 van de verordening dan ook vrij om de nationale stelsels voor elektronische identificatie bij de Europese Commissie aan te melden. Zolang Nederland geen stelsel dat op nationaal niveau wordt gebruikt aanmeldt, kunnen gebruikers met een Nederlands middel niet met een beroep op de verordening inloggen bij diensten in een andere lidstaat, waarvoor identificatie vereist is onder de voorwaarden die de desbetreffende lidstaat daaraan stelt. Veelal kan dit dan alleen met behulp van een identificatiemiddel uit die desbetreffende lidstaat.

3.2 Voorgestelde uitvoering eidas-verordening op hoofdlijnen

De leden van de D66-fractie informeerden of het knooppunt dat dient tot grensoverschrijdende acceptatie van elektronische identificatiemiddelen in september 2018 ook daadwerkelijk gereed zal zijn. Het antwoord op deze vraag is bevestigend. Een eerste versie van het eIDAS-knooppunt is reeds gereed en wordt momenteel voor proefprojecten gebruikt. Deze zal in 2017 vervangen worden door de referentie-implementatie van het eIDAS-knooppunt. De Europese Commissie heeft de software daarvoor inmiddels opgeleverd. Op dit moment kunnen de eIDAS-knooppunten van 16 landen met elkaar communiceren. Er worden nu proefprojecten gedaan in het kader van de implementatie van de eIDAS-verordening. Door koppeling van het Nederlandse eIDAS-knooppunt aan het Belgische knooppunt kunnen Belgische grensboeren met hun Belgische elektronische identificatiemiddel op de website mijn.RVO.nl inloggen om gebruik te maken van agrarische regelingen in Nederland. Tegelijkertijd kunnen Nederlandse grensboeren hetzelfde doen bij landbouwvlaanderen.be. Er wordt gewerkt aan de aansluiting van Nederland met meer landen, zoals Duitsland.

De leden van de D66-fractie wilden weten of er al een aanbestedingsprocedure voor het eIDAS-knooppunt is gestart. Het antwoord op deze vraag is ontkennend. De ontwikkeling van het knooppunt vindt op dit moment in eigen beheer door het Ministerie van Economische Zaken plaats (Dienst ICT Uitvoering), zodat er geen aanbestedingsprocedure hiervoor heeft plaatsgevonden. De Minister van Economische Zaken is en blijft daarmee verantwoordelijke voor het eIDAS-knooppunt in de zin van de Wet Bescherming Persoonsgegevens (artikel 1d).

De leden van de D66-fractie wilden weten of de regering zich bewust is van de complexiteit van zowel de ontwikkeling als het onderhoud van een dergelijk knooppunt, zoals genoemd in het advies van het Cbp. Het antwoord hierop is bevestigend. De ontwikkeling van een eIDAS-knooppunt is niet eenvoudig en vereist een zorgvuldige ontwikkeling en aandacht voor ook het onderhoud van een dergelijk knooppunt.

Bescherming van persoonsgegevens, het hanteren van voldoende en eenduidige beveiligingsmaatregelen en verantwoordelijkheidsverdeling binnen ketens, zijn bijvoorbeeld belangrijke aandachtspunten. Met de ontwikkeling van het eIDAS-knooppunt is dan ook tijdig aangevangen, waarbij een eerste «Privacy Impact Assesment» is uitgevoerd en waarover de Autoriteit persoonsgegevens (voorheen: Cbp) heeft geadviseerd. In dat advies heeft de Autoriteit persoonsgegevens onder meer gewezen op het feit dat de ontwikkeling van het eIDAS-knooppunt complex is, en dat het grondrecht voor bescherming van de persoonlijke levenssfeer voldoende gewaarborgd moet zijn. Mede vanwege deze complexiteit zal het knooppunt voorlopig in beheer van de Minister van Economische Zaken blijven en onder zijn verantwoordelijkheid worden doorontwikkeld. De aanbeveling van de Autoriteit persoonsgegevens om bij de verdere ontwikkeling van het knooppunt aanvullende «Privacy impact assessments» uit te laten voeren wordt overgenomen.

De leden van de D66-fractie vroegen zich af op welke manier het advies van het Cbp wordt meegenomen in de ontwikkeling van het eIDAS-knooppunt. In de beantwoording van de vorige vragen in deze paragraaf van deze leden is reeds op de verwerking van het advies ingegaan. Het advies om bij de doorontwikkeling Privacy Impact Assessments uit te voeren wordt overgenomen. Daarnaast is de verantwoordelijkheid voor het eIDAS-knooppunt een belangrijk punt uit het Cbp-advies. Het knooppunt blijft in ieder geval tot september 2018 in beheer van de Minister van Economische Zaken. Daarmee blijft de Minister voorlopig zowel beheerder als verantwoordelijke voor het eIDAS-knooppunt in de zin van de Wet Bescherming Persoonsgegevens (artikel 1d). Op korte termijn is te verwachten dat het aantal transacties te overzien is waardoor één knooppunt volstaat. Op langere termijn kan het hebben van één knooppunt risico's inhouden. Bijvoorbeeld doordat het vanwege technische problemen kan uitvallen, waardoor geen grensoverschrijdende authenticatie meer mogelijk is of vanwege aanvallen. Het hebben van één knooppunt is enerzijds overzichtelijk qua beveiliging en beheer maar betekent anderzijds een mogelijk «single point of failure». Een oplossing zou kunnen zijn om meerdere knooppunten te creëren. Wanneer hiervoor zou worden gekozen, wordt het advies van de Autoriteit Persoonsgegevens opgevolgd door duidelijk aan te wijzen wie verantwoordelijken zijn voor de knooppunten. De Minister van Economische Zaken blijft verantwoordelijke in de zin van de Wet bescherming persoonsgegevens voor het bestaande knooppunt. Daarbij hoort het afsluiten van een bewerkersovereenkomst waarin onder meer de beveiliging wordt geregeld.

4. Erkenning elektronische identificatiemiddelen

4.1 Grensoverschrijdende erkenning elektronische identificatiemiddelen

De vraag van de leden van de PvdA-fractie of het klopte dat de rechtsgevolgen van de gekwalificeerde elektronische handtekening tot nu toe worden geregeld in artikel 3:15a van het Burgerlijk Wetboek kan bevestigend worden beantwoord.
Art. 3:15a bepaalt thans in het eerste lid dat een elektronische handtekening dezelfde rechtsgevolgen heeft als een handgeschreven handtekening indien de methode die daarbij gebruikt is voor authentificatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval. Dit lid ziet zowel op de gekwalificeerde elektronische handtekening, de geavanceerde elektronische handtekening en de andere (gewone) elektronische handtekening.

Deze leden wilden verder weten waarom het rechtsgevolg van de gekwalificeerde elektronische handtekening wordt geschrapt. De aanleiding is dat de verordening in artikel 25, tweede lid, zelf het rechtsgevolg van de gekwalificeerde handtekening bepaalt. De verordening schrijft voor dat zo'n handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. Daardoor is er voor de lidstaten geen noodzaak, maar ook geen ruimte meer om dit rechtsgevolg te regelen. Voor de geavanceerde elektronische handtekening en de andere elektronische handtekeningen geldt dat deze wel door de lidstaten kunnen worden bepaald. Daarom is in het gewijzigde artikel 3:15a BW thans alleen een regeling met betrekking tot de rechtsgevolgen van deze beide categorieën handtekeningen opgenomen.

De leden van de PvdA-fractie informeerden naar de verschillen en overeenkomsten tussen elektronische handtekeningen, geavanceerde elektronische handtekeningen en gekwalificeerde elektronische handtekeningen. De overeenkomst tussen elektronische handtekeningen, geavanceerde en gekwalificeerde elektronische handtekeningen is dat het steeds gaat om elektronische gegevens (de handtekening) die verbonden worden aan andere elektronische gegevens, bijvoorbeeld een document. De functie van de handtekening is steeds dezelfde namelijk dat de ondertekenaar aangeeft de inhoud van het document te kennen en met zijn handtekening zijn wil kenbaar maakt. De elektronische handtekening is vormvrij en kan eenvoudig zijn, zoals een met een pen gezette gescande handtekening. Een geavanceerde handtekening voldoet aan vier eisen die in de verordening staan. Deze eisen waarborgen dat de handtekening doorgaans betrouwbaarder en veiliger is dan de vormvrije elektronische handtekening. Een eis is bijvoorbeeld dat wijziging van de gegevens, zoals die in een document, na ondertekening opgespoord moet kunnen worden. De geavanceerde handtekening zal worden gevraagd wanneer er een hogere zekerheid vereist is. Een gekwalificeerde elektronische handtekening is een geavanceerde handtekening die voldoet aan twee extra in de verordening bepaalde eisen. De eerste eis is dat bij ondertekening gebruik moet worden gemaakt van een zogeheten gekwalificeerd middel. Dit kan hardware, zoals een beveiligde smartcard of USB-stick, of speciale software zijn. De tweede eis is dat de handtekening gebaseerd moet zijn op een gekwalificeerd certificaat voor elektronische handtekeningen. De combinatie van gekwalificeerd middel en gekwalificeerd certificaat levert een zeer hoge mate van betrouwbaarheid op dat het document daadwerkelijk is ondertekend door de eigenaar van de elektronische handtekening. Welke handtekening het meest geschikt is voor een procedure of transactie hangt af van de risico's. Naarmate de risico's groter zijn, is het verstandiger om een handtekening met een hoger betrouwbaarheidsniveau te gebruiken. Om de uitvoering te helpen om de juiste handtekening bij een digitaal proces te kiezen, heeft het Forum Standaardisatie een handreiking ontwikkeld: https://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_v3__2014_.pdf

De leden van de PvdA-fractie vroegen welke technische verschillen er met betrekking tot elektronische handtekeningen zijn en welke verschillen er in rechtsgevolgen zijn.
De «gewone» elektronische handtekening is vormvrij en het zetten van een dergelijke handtekening gebeurt meestal in de gebruiksomgeving waar de ondertekenaar zich bevindt. Hiervoor zijn doorgaans geen aparte technische voorzieningen nodig. Voor een geavanceerde handtekening kan de techniek van digitale certificaten worden gebruikt, maar dit hoeft niet. Voor grensoverschrijdende acceptatie is het van belang dat deze handtekening voldoet aan een in een uitvoeringshandeling vastgestelde elektronisch formaat. Het gaat dan om een technisch formaat dat door mensen of computers leesbaar moet zijn (CAdeS, PAdES, XAdES en

ASiC). Gekwalificeerde handtekeningen werken met de techniek van Public Key Infrastucture (PKI). Technisch gezien zijn de belangrijkste verschillen dat bij gekwalificeerde elektronische handtekeningen zwaardere eisen worden gesteld aan de cryptografische algoritmes en sleutellengtes en aan de technische beveiliging ter plekke van de vertrouwensdienstverlener. Daarnaast kent het uitgifteproces meer waarborgen waardoor er sprake is van een hoge betrouwbaarheid. Met betrekking tot de rechtsgevolgen kan het volgende worden aangegeven. Zoals hiervoor opgemerkt bepaalt de verordening in artikel 25, tweede lid, dat een gekwalificeerde handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. De rechtsgevolgen van de geavanceerde en de andere (gewone) handtekeningen zijn ter bepaling aan de lidstaten. In het gewijzigde artikel 3:15a is aangesloten bij de huidige regeling over de rechtsgevolgen en is bepaald dat een elektronische geavanceerde en een andere elektronische handtekening dezelfde rechtsgevolgen hebben als een handgeschreven handtekening indien de methode die daarbij gebruikt is voor ondertekening voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval. Voor deze handtekeningen geldt derhalve de toets van voldoende betrouwbaarheid.

De leden van de PvdA-fractie vroegen voorts met betrekking tot de elektronische handtekening van artikel 2:16 Awb hoe wordt bepaald of deze voldoende betrouwbaar is, in welke nadere regelgeving dit wordt vastgesteld en waar zal worden geregeld welke aanvullende eisen zullen worden gesteld. Het voorgestelde artikel 2:16, eerste lid, Awb stelt buiten twijfel dat aan het vereiste van ondertekening niet alleen kan worden voldaan door een handgeschreven handtekening, maar ook door een elektronische handtekening. De zinsnede met betrekking tot de betrouwbaarheid is overgenomen uit het huidige artikel 2:16 Awb. De toelichting op deze bepaling vermeldde destijds dat de mate van betrouwbaarheid en vertrouwelijkheid die wordt vereist, kan variëren. De neiging bestaat bij elektronisch verkeer een hogere mate van betrouwbaarheid en vertrouwelijkheid te eisen dan bij conventionele communicatie. Dit is niet gewenst, want ook de handtekening op papier biedt geen absolute garanties tegen vervalsingen. Er zijn in theorie drie maten van betrouwbaarheid en vertrouwelijkheid te onderscheiden:

- Van maximale betrouwbaarheid en vertrouwelijkheid is sprake indien de beveiliging geheel conform de maximaal (technische) mogelijkheden plaatsvindt.
- Van voldoende betrouwbaarheid en vertrouwelijkheid is sprake indien de veiligheid even groot is vergeleken met de situatie dat er uitsluitend van conventioneel verkeer gebruik zou worden gemaakt.
- Van pro forma betrouwbaarheid en vertrouwelijkheid is sprake indien de beveiliging slechts één stap verwijderd is van het bieden van geen enkele beveiliging; zij bestaat bijvoorbeeld uit de (elektronische) mededeling «verboden toegang».

Absolute betrouwbaarheid en vertrouwelijkheid bestaan niet. De maximale betrouwbaarheid en vertrouwelijkheid zijn afhankelijk van de stand der techniek en de (financiële) inspanningen die men er voor over heeft. Pro forma betrouwbaarheid en vertrouwelijkheid zal doorgaans onvoldoende zijn. Het ligt in de rede ervan uit te gaan dat elektronisch verkeer even betrouwbaar en vertrouwelijk moet zijn als conventioneel verkeer. Dit betekent dat gestreefd moet worden naar een voldoende mate van betrouwbaarheid en vertrouwelijkheid. Dit is in het huidige artikel 2:16 Awb tot uitdrukking gebracht door een voldoende mate van betrouwbaarheid en vertrouwelijkheid te vereisen (zie ook Kamerstukken II 2001/02, 28 483, nr. 3, p. 16–17). Dit wetsvoorstel brengt hierin geen verandering.

Wanneer precies sprake is van voldoende mate van betrouwbaarheid en vertrouwelijkheid is in algemene zin moeilijk te zeggen. In sommige gevallen van uitwisseling van informatieve berichten is er weinig behoefte aan bescherming. Een e-mailbericht zonder een elektronische handtekening of een sms-bericht kan al voldoende zijn. In andere gevallen – als de aard en inhoud van het bericht daartoe aanleiding geven – bestaat er wel behoefte aan meer bescherming. Zo moeten aan de verlening van een vergunning hogere eisen worden gesteld dan aan de verstrekking van algemene inlichtingen die ook langs andere kanalen verkrijgbaar zijn. De Verordening bepaalt dat een gekwalificeerde handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. Het gebruik van een gekwalificeerde elektronische handtekening is derhalve altijd voldoende betrouwbaar. Voor geavanceerde en gewone elektronische handtekeningen geldt dat om te beoordelen of in een bepaald geval een elektronische handtekening voldoende betrouwbaar is, dient te worden gelet op de aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt. Indien gelet op deze omstandigheden sprake is van een voldoende betrouwbare handtekening, heeft deze hetzelfde rechtsgevolg als een handgeschreven handtekening en kan deze derhalve niet door een bestuursorgaan worden geweigerd (zie ook paragraaf 6.1 en 6.2 van de memorie van toelichting).

Het tweede lid van artikel 2:16 Awb maakt het mogelijk om het gebruik voor te schrijven van hetzij de gewone, hetzij de geavanceerde, hetzij de gekwalificeerde elektronische handtekening. Aan deze mogelijkheid kan behoefte zijn in het licht van het doel waarvoor de elektronische gegevens worden gebruikt, de aard van de rechtsverhouding tussen de ondertekenaar en het bestuursorgaan of andere omstandigheden van het geval. Dit voorschrijven gebeurt door de centrale overheid bij of krachtens een wet of door een ander bestuursorgaan met regelgevende bevoegdheid in de eigen verordening. Als het gebruik van de gewone elektronische handtekening wordt voorgeschreven, kunnen in de regeling waarin dit gebruik wordt voorgeschreven, nadere eisen worden gesteld. Met deze eisen kan de veiligheid en betrouwbaarheid van de ondertekening door middel van deze handtekening worden verzekerd. Gedacht kan bijvoorbeeld worden aan eisen aan het niveau van authenticatie op basis waarvan de elektronische handtekening wordt aangemaakt of eisen aan de onafhankelijkheid en veiligheid van het mechanisme waarmee de gegevens die dienen ter ondertekening, worden gehecht aan het te ondertekenen document, bericht of de gestandaardiseerde gegevensset. Ook kunnen er bijvoorbeeld aanvullende eisen worden gesteld aan de elektronische handtekening die door middel van een tablet wordt gezet. In dit verband kan hoofdstuk 9 over ondertekenen van de Handreiking voor overheidsorganisaties van het Forum Standaardisatie als leidraad dienen (Forum Standaardisatie, Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, versie 3, augustus 2014).

De leden van de SP-fractie vroegen naar de risico's van middelen met minimaal het substantiële betrouwbaarheidsniveau en informeerden naar een voorbeeld van een dienst die zich aan de onderkant bevindt van het substantiële betrouwbaarheidsniveau.
Het risico van middelen met het betrouwbaarheidsniveau substantieel zit onder meer in het uitgifteproces. De eisen hiervoor zijn lager dan bij het hoge niveau. Het risico is dat een persoon een elektronisch identificatiemiddel namens een ander kan bemachtigen, hetgeen tot identiteitsfraude kan leiden. Door het gebruik van tweefactorauthenticatie, waarbij de benodigde factoren los van elkaar worden aangemaakt en verstrekt, kan het risico op misbruik worden verkleind. Er is op dit moment in Nederland nog geen dienst aan te wijzen die zich aan de onderkant bevindt van het substantieel betrouwbaarheidsniveau.

De leden van de PVV-fractie waren benieuwd op welke manier het Agentschap Telecom gaat toetsen of een buitenlands elektronisch identificatiemiddel aan de afspraken ten aanzien van de betrouwbaarheidsniveaus voldoet. Deze leden wilden ook weten of de Nederlandse toezichthouder verder niet meer controleert, nadat een stelsel voor elektronische identificatie van een ander land de status van hoge betrouwbaarheid heeft behaald. De verordening geeft de nationale toezichthouders geen bevoegdheden ten aanzien van elektronische identificatiemiddelen. Het Agentschap Telecom kan elektronische identificatiemiddelen uit andere lidstaten dan ook niet toetsen aan betrouwbaarheidseisen van de verordening. De erkenning van een buitenlands elektronisch identificatiemiddel vindt plaats in een bij de Europese Commissie te doorlopen aanmeldingsprocedure op grond van de eerder aangehaalde Uitvoeringsverordening. In die procedure wordt het stelsel van elektronische identificatie aangemeld dat de basis vormt voor de uitgifte van de elektronische identificatiemiddelen, waarbij allerlei informatie moet worden verstrekt waaronder ook over de nationale van toepassing zijnde toezichtregeling, informatie over de aansprakelijkheidsregeling van de betrokken partijen en beschrijving van het betrouwbaarheidsniveau. Om beter inzicht te verkrijgen in de inrichting van aangemelde stelsels uit andere lidstaten en daarop gezamenlijk als lidstaten te kunnen reflecteren om de kwaliteit daarvan te verbeteren en van elkaar te leren bevat de verordening voorschriften over samenwerking tussen lidstaten, die zijn uitgewerkt in Uitvoeringsverordening 2015/296 van de Europese Commissie van 24 februari 2015 tot vaststelling van procedurele voorschriften betreffende de samenwerking tussen de lidstaten op het gebied van elektronische identificatie overeenkomstig artikel 12, lid 7, van Verordening (EU) nr. 910/2014 (PbEU L53/14). Deze samenwerking strekt zich uit tot de veiligheid van de stelsels voor elektronische identificatie, de uitwisseling van informatie, ervaring en goede werkwijzen van aangemelde stelsels, de technische vereisten inzake zowel het niveau van betrouwbaarheid als het werken daarmee, en onderzoek naar ontwikkelingen in de sector. Onderdeel van die samenwerking is ook de zogeheten «onderlinge evaluatie», die ruimte laat voor een kritische houding van lidstaten jegens een andere lidstaat indien daarvoor aanleiding bestaat, ook nadat aanmelding heeft plaatsgevonden. Wel moet de lidstaat die het stelsel van een andere lidstaat opnieuw wil evalueren, aangeven waarom een nieuwe of aanvullende onderlinge evaluatie nodig is en op welke manier dit zou bijdragen aan de interoperabiliteit of de veiligheid. Nederlandse deskundigen hebben de mogelijkheid om mee te doen aan deze onderlinge evaluatie. De bevindingen van deze evaluatie worden gedeeld in de zogeheten samenwerkingsgroep. De samenwerkingsgroep brengt een advies uit dat moet worden vermeld op het notificatieformulier van de Commissie. Het is vervolgens de Europese Commissie die een stelsel plaatst op de lijst met aangemelde stelsels.

4.2 Uitvoeringsmaatregelen

De leden van de PvdA-fractie vroegen naar de stand van zaken met betrekking tot het eIDAS-knooppunt, dat in september 2018 gereed zou zijn. Het antwoord op deze vraag is opgenomen in de beantwoording van vergelijkbare vragen van de leden van de D66-fractie hierover in paragraaf 3.2.

De leden van de PvdA-fractie informeerden wanneer de bijbehorende Privacy Impact Assessments aan de Kamer wordt verstuurd. Bij deze nota naar aanleiding van het verslag is de eerder uitgevoerde «Privacy Impact

Assesment» als bijlage bijgevoegd[1]. Desgewenst zal een aanvullende «Privacy Impact Assessment», wanneer deze gereed is ook worden toegezonden aan de Kamer.

De leden van de PvdA-fractie wilden verifiëren of het Cbp geadviseerd heeft een Privacy Impact Assessment uit te voeren. De uitvoering van een eerste «Privacy Impact Assessment» is op eigen initiatief van het Ministerie van Economische Zaken tot stand gekomen. In het kader van de advisering over het wetsvoorstel aan de Autoriteit persoonsgegevens is de «Privacy Impact Assessment» vervolgens aan de Autoriteit persoonsgegevens toegezonden. Omdat ten tijde van de eerste «Privacy Impact Assessment» nog niet alles was uitgekristalliseerd hebben zowel de opstellers van de eerste «Privacy Impact Assessment» als de Autoriteit persoonsgegevens aangeraden om aanvullende «Privacy Impact Assessments» uit te voeren. Dit advies wordt opgevolgd.

De leden van de PvdA-fractie wilden weten of de aanvullende «Privacy Impact Assessments» inmiddels beschikbaar zijn of dat die nog worden uitgevoerd en zo ja, wanneer die beschikbaar zijn. In de beantwoording van de vorige vraag van de PvdA-fractie is reeds ingegaan op de «Privacy Impact Assessments». Zoals daar te lezen is, is een eerste aanvullende «Privacy Impact Assessment» nog niet uitgevoerd. De reden daarvan is dat op dit moment gewerkt wordt aan de architectuur van de inbedding van het eIDAS-knooppunt in de nationale stelsels voor elektronische identificatie. Zodra dit gereed is, zal de eerste aanvullende «Privacy Impact Assessment» in de zomer van 2016 worden uitgevoerd en in het najaar beschikbaar zijn. Desgewenst worden de resultaten daarvan naar de Tweede Kamer gezonden.

De leden van de PvdA-fractie informeerden waar het eIDAS-knooppunt wordt ingericht. De ontwikkeling van het knooppunt vindt in eigen beheer door het Ministerie van Economische Zaken plaats (Dienst ICT Uitvoering). De daarvoor benodigde ICT-voorzieningen bevinden zich fysiek in het rijksoverheid Datacenter (ODC) Noord in Groningen. In antwoord op een eerdere vraag van de leden van de D66-fractie in paragraaf 3.2 is aangegeven dat het knooppunt in ieder geval tot september 2018 in beheer van de Minister van Economische Zaken blijft en dat deze zowel beheerder als verantwoordelijke is in de zin van de Wet Bescherming Persoonsgegevens is (artikel 1d). Wanneer daarna wordt gekozen voor het onderbrengen van het knooppunt bij een makelaar uit een stelsel voor elektronische identficatie, dan verwerkt deze de persoonsgegevens slechts als bewerker in de zin van de Wet bescherming persoonsgegevens in opdracht en onder de verantwoordelijkheid van de Minister.

De leden van de PvdA-fractie vroegen welke landen aangesloten moeten zijn op het eIDAS-knooppunt. Alle lidstaten van de Europese Unie hebben de verplichting de verordening uit te voeren, inclusief de daarop berustende Uitvoeringsverordening (EU) nr. 2015/1501 van de Commissie van 8 september 2015 betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van de verordening (PbEU 2015, L235) (hierna: Uitvoeringsverordening over eIDAS-knooppunten). Alle lidstaten dienen op grond hiervan gebruik te maken van een eIDAS-knooppunt. Op 29 augustus 2014 heeft de Europese Vrijhandelsassociatie (EVA) namens de landen van de Europese Economische Ruimte de verordening in behandeling genomen (http://www.efta.int/eea-lex/32014R0910). Naar verwachting zal de verplichting tot gebruik van knooppunten ook op IJsland, Liechtenstein en Noorwegen gaan rusten.

[1] Raadpleegbaar via www.tweedekamer.nl

De leden van de PvdA-fractie wilden expliciet weten of ook Roemenië en Bulgarije aangesloten worden op het eIDAS-knooppunt. Om de erkenning van elektronische identificatiemiddelen mogelijk te maken heeft iedere lidstaat een knooppunt nodig. Dit geldt dus ook voor Roemenië en Bulgarije.

De leden van de PvdA-fractie vroegen wat er gebeurt als de toekenning van elektronische identiteiten in landen als Roemenië en Bulgarije lek is (d.w.z. vervalste identiteiten, identiteitsdiefstal, etc.)? Een lidstaat die een stelsel voor elektronische identificatiemiddelen heeft aangemeld, dient de Europese Commissie en de andere lidstaten te informeren over veiligheidsproblemen met elektronische identiteiten van een aangemeld stelsel. De lidstaat die het stelsel heeft aangemeld is verplicht bij een veiligheidsinbreuk of integriteitsverlies de grensoverschrijdende authenticatie onverwijld geheel of gedeeltelijk op te schorten of in te trekken (artikel 10, van de verordening). Nederlandse openbare instanties ontvangen dan niet langer verzoeken met gebruikmaking van elektronische identificatiemiddelen van het gecompromitteerde stelsel. Indien de inbreuk of schending niet binnen drie maanden na deze opschorting of intrekking is verholpen, stelt de aanmeldende lidstaat de andere lidstaten en de Commissie op de hoogte van de intrekking van het stelsel voor elektronische identificatie.

De leden van de PvdA-fractie vragen voorts of hiermee geen identificatieproblemen van andere landen in Nederland worden geïmporteerd. Het is in de eerste plaats de verantwoordelijkheid van de lidstaten zelf die een stelsel hebben aangemeld bij de Europese Commissie er voor te zorgen dat dit stelsel niet kwetsbaar is voor identiteitsvervalsing of -diefstal. De verordening voorziet zoals in antwoord op de vorige vraag van de leden van de PvdA-fractie is aangegeven in een procedure tot schorsing en uiteindelijk intrekking van een stelsel met veiligheidsproblemen. Het is in het belang van een lidstaat zelf dat het zover niet komt met het oog op het functioneren van eigen elektronische processen waarvoor identificatie vereist is, maar ook omdat burgers en ondernemers van die lidstaat anders niet langer langs digitale weg administratieve procedures met openbare instanties in andere lidstaten nog kunnen afwikkelen. Voorts bevat de verordening voorschriften over samenwerking en interoperabiliteit tussen lidstaten, die ruimte laten voor een kritische houding van lidstaten jegens een andere lidstaat indien daarvoor aanleiding bestaat. Deze samenwerking strekt zich uit tot de veiligheid van de stelsels voor elektronische identificatie, de uitwisseling van informatie, ervaring en goede werkwijzen van aangemelde stelsels, de technische vereisten inzake zowel het niveau van betrouwbaarheid als het werken daarmee, onderlinge evaluatie van aangemelde stelsels en onderzoek naar ontwikkelingen in de sector. Deze vorm van verplichte samenwerking biedt mogelijkheden om beter inzicht te verkrijgen in de inrichting van aangemelde stelsels uit andere lidstaten en daarop gezamenlijk als lidstaten te kunnen reflecteren om de kwaliteit daarvan te verbeteren en van elkaar te leren.

De leden van de PvdA-fractie vragen of inmiddels zeker is gesteld dat het knooppunt dat grensoverschrijdende identificatie mogelijk maakt geen gegevens kan en mag opslaan. Het realiseren van het knooppunt is onderdeel van de feitelijke uitvoering van de verordening ten behoeve van de wederzijdse erkenning van elektronische identificatiemiddelen tussen lidstaten en geen onderdeel van het wetsvoorstel zelf. Het knooppunt is onderwerp van de eerder aangehaalde Uitvoeringsverordening over eIDAS-knooppunten. In deze uitvoeringsverordening is voorgeschreven dat een knooppunt geen identiteitsgegevens mag opslaan, behalve gegevens aan de hand waarvan, in geval van een incident, de uitwisseling van berichten in de juiste volgorde kan worden gereconstrueerd teneinde

de plaats en de aard van het incident vast te stellen. Deze gegevens worden zolang bewaard als volgens de nationale voorschriften vereist is en bevatten ten minste de identificatie van het knooppunt, de identificatie van het bericht en de datum en de tijd van het bericht (artikel 6, tweede lid, juncto artikel 9, derde lid, van de desbetreffende Uitvoeringsverordening). Bij de ontwikkeling van het knooppunt zullen deze loggegevens worden vastgelegd om incidenten te kunnen reconstrueren, overeenkomstig en met inachtneming van het daaromtrent bepaalde in deze uitvoeringsverordening. Voor het overige zullen persoonsgegevens en eventuele andere gegevens via het knooppunt worden doorgeleid, versleuteld en kortstondig in het knooppunt worden opgeslagen. Dit is noodzakelijk om de werking van het knooppunt ten behoeve van grensoverschrijdende elektronische identificatie en authenticatie mogelijk te maken. Er worden hiermee niet meer (persoons)gegevens opgeslagen dan nodig is voor een goede uitvoering van de verordening met behulp van het knooppunt.

De leden van de PvdA-fractie vroegen op welke wijze storingen bij het eIDAS-knooppunt ondervangen worden. Een storing in het knooppunt maakt grensoverschrijdend gebruik van elektronische identiteiten tijdelijk niet mogelijk. Hierdoor kunnen diensten niet meer elektronisch worden verleend en kan er mogelijk schade ontstaan. Een burger of bedrijf mag hiervan niet de dupe worden. Een mogelijkheid om storingen met het knooppunt te ondervangen is het inrichten van meerdere knooppunten. Een ander knooppunt kan de taak van een knooppunt dan overnemen in geval van storing. Het inrichten van meerdere knooppunten verhoogt de zekerheid van dienstverlening maar kent veiligheidsrisico's. Ieder knooppunt kent veiligheidsrisico's en meerdere knooppunten betekent meer kans dat er iets mis gaat.

De leden van de SP-fractie begrepen dat via het met deze wet ingestelde knooppunt verbinding kan worden gemaakt met het nationale stelsel voor elektronische identiteiten. Deze leden wilden informatie over de risico's die een buitenlands middel met betrouwbaarheidsniveau «laag» met zich mee kan brengen. Het risico van een middel met betrouwbaarheidsniveau laag is dat het mogelijk is om dit op naam van iemand anders aan te vragen en te gebruiken. Als dat gebeurt is er sprake van identiteitsfraude. Doordat voor middelen met lage betrouwbaarheidsniveau lichtere eisen gelden aan het aanvraagproces, beheer en uitgifte is het risico op onrechtmatige verkrijging en gebruik hoger dan bij middelen van met een substantieel of hoog betrouwbaarheidsniveau. De verordening verplicht overigens niet tot erkenning van middelen met betrouwbaarheidsniveau laag. Lidstaten kunnen er zelf voor kiezen om deze van elkaar te accepteren.

De leden van de SP-fractie informeerden welke mogelijkheden er zijn om het identificatiemiddel op het niveau «laag» te weren, welke voorzorgsmaatregelen hiertegen worden voorbereid, en op welke wijze de Minister van Economische Zaken met de Minister van Binnenlandse Zaken zal samenwerken om deze risico's uit te bannen. Zoals in het antwoord op de vorige vraag van deze leden is aangegeven, verplicht de verordening niet tot erkenning van middelen met een laag betrouwbaarheidsniveau. Nederland kan alle middelen uit andere lidstaten met dit betrouwbaarheidsniveau dan ook weren. Nederland is niet voornemens om middelen met betrouwbaarheidsniveau laag uit andere lidstaten te accepteren. Voorzorgsmaatregelen om mogelijke risico's die met middelen van niveau laag samenhangen te ondervangen zijn dan ook niet nodig.

De leden van de PVV-fractie wilden weten waarom de Kamer wordt gevraagd om in te stemmen met erkenning van elektronische identificatiemiddelen van andere Europese lidstaten, terwijl de benodigde technische voorziening nog gerealiseerd moet worden en de Kamer nog moet beslissen of het nieuwe eID-stelsel wenselijk is en vraagt naar de reikwijdte hiervan. De Kamer wordt gevraagd in te stemmen met het wetsvoorstel dat de noodzakelijke aanpassingen regelt van Nederlandse wetgeving om aan de verordening te voldoen. Die aanpassingen hebben betrekking op vertrouwensdiensten. Daarnaast regelt de verordening met rechtstreekse werking de grensoverschrijdende erkenning van elektronische identificatiemiddelen door openbare instanties. De verordening bepaalt in artikel 52 lid 2c dat deze wederzijdse erkenning vanaf september 2018 verplicht is. Om aan die in de verordening zelf vastgelegde verplichting feitelijk te kunnen voldoen, is het nodig dat er binnen twee jaar een eIDAS-knooppunt wordt opgeleverd. Nederland heeft al een eerste testversie van het knooppunt opgeleverd. Inmiddels heeft de Europese Commissie een eerste versie van implementatieprogrammatuur voor het eIDAS-knooppunt opgeleverd die de testversie vervangt. De komende tijd zal worden gewerkt aan aansluiting van een of meer nationale stelsels voor elektronische identificatie op het eIDAS-knooppunt. Het voordeel van aansluiting is dat Nederlandse openbare instanties geen aparte aansluiting op het knooppunt hoeven te realiseren. Het stelsel handelt dan zowel het nationale als internationale gebruik van elektronische identificatie en authenticatie van burgers en bedrijven af.

4.3 De melding van een stelsel tot bewerkstelliging van erkenning

De leden van de D66-fractie vroegen naar duiding van de zinsnede uit de verordening «de aanmeldende lidstaat [dient] te voorzien in de werking en beschikbaarheid van een online authenticatievoorziening» en wilden weten of elke lidstaat nu apart in een authenticatievoorziening, een knooppunt, moet voorzien. Met de online authenticatievoorziening wordt inderdaad het eIDAS-knooppunt bedoeld. Via de eIDAS-knooppunten worden de nationale elektronische identificatie-infrastructuren bruikbaar gemaakt voor openbare instanties in andere lidstaten. Dit impliceert dat elke lidstaat één of meer aparte eIDAS-knooppunt(en) heeft.

De leden van de D66-fractie informeerden of de regering mogelijkheden ziet om het aanbesteden van een dergelijk knooppunt via open source software te laten verrichten. Op deze manier hoeft niet 28 keer dezelfde software te worden aanbesteed. Voor implementatie van het knooppunt wordt door de Europese Commissie programmatuur beschikbaar gesteld. Dit mag, maar hoeft een lidstaat niet te gebruiken bij het inrichten van een eIDAS-knooppunt. Deze programmatuur is gebaseerd op «open source software. Het voornemen is van deze «open source software» gebruik te maken voor het eIDAS-knooppunt in Nederland.
De leden van de D66-fractie vroegen of het overwogen is of zelfs mogelijk, om in plaats van 28 afzonderlijke knooppunten één knooppunt te creëren. Theoretisch is het mogelijk om één Europees knooppunt te creëren dat het berichtenverkeer voor grensoverschrijdende authenticatie voor alle lidstaten afhandelt. Een dergelijk knooppunt is onwenselijk omdat dit een zeer aantrekkelijk doelwit zou worden voor aanvallen. Als het centrale knooppunt uit zou vallen, zou de grensoverschrijdende authenticatie compleet stilvallen.

4.4 Uitvoeringsmaatregelen

De leden van de D66-fractie stelden vast dat er nog geen uitsluitsel is over de vraag of en wanneer Nederland een stelsel voor elektronische identificatie gaat aanmelden en vroegen zich af welke middelen voor een

dergelijk stelsel in aanmerking komen en in hoeverre dit samenhangt met het nationale stelsel voor elektronische identificatiemiddelen en welke andere nationale ontwikkelingen invloed hebben op een eventuele Nederlandse aanmelding voor wederzijdse erkenning. Er is inderdaad nog geen besluit genomen over de aanmelding van een of meerdere nationale stelsels voor elektronische identificatiemiddelen. Indien er sprake zou zijn van aanmelding dan omvat deze alle middelen van het aangemelde stelsel die het niveau substantieel of hoog hebben. Deze middelen zijn nationaal nog niet breed uitgerold. Voor burgers ontwikkelt de Minister van Binnenlandse Zaken en Koninkrijksrelaties een identificatiemiddel op niveau hoog. Andere nationale ontwikkelingen die invloed hebben op een Nederlandse aanmelding zijn de behoefte van burgers en bedrijven om de Nederlandse elektronische identificatiemiddelen grensoverschrijdend te gebruiken. Deze behoefte hangt, naast de beschikbaarheid van middelen op het niveau substantieel en hoog, samen met het aanbod van voor Nederlandse burgers en bedrijven aantrekkelijke diensten in andere lidstaten. De verwachting is dat dit aanbod de komende jaren beperkt zal blijven.

5. Het verlenen van vertrouwensdiensten

5.3 Meldplichten bij inbreuk op veiligheid of verlies van integriteit

De leden van de D66-fractie verzochten om het begrip «aanzienlijk» bij het melden van een veiligheidsinbreuk of integriteitsverlies te definiëren. Het begrip «aanzienlijk» is een open norm uit de verordening. Het melden van inbreuken zonder «aanzienlijke» gevolgen is met het oog op de beperking van administratieve lasten niet wenselijk. Er dient niet te snel te worden aangenomen dat een melding op grond van de verordening achterwege kan blijven met als reden dat aanzienlijke gevolgen ontbreken. Gelet op de ernst en omvang van de gevolgen die een incident met vertrouwensdiensten kan veroorzaken, wordt aangenomen dat de verordening hierin ruim opgevat dient te worden. Dat wil zeggen dat ook sprake is van aanzienlijke gevolgen als bedoeld in de verordening indien een incident aanzienlijke gevolgen voor de verleende vertrouwensdienst kan hebben, ongeacht of het zeker is dat die zullen intreden. En in geval van gerede twijfel over de vraag hoe groot de gevolgen daadwerkelijk kunnen zijn, dient eveneens tot melding te worden overgegaan. Wanneer de betrouwbaarheid en daarmee rechtszekerheid van transacties in het geding is of een kans op identiteitsfraude voor meerdere personen bestaat doordat sleutels in verkeerde handen gevallen zijn, zal er sprake zijn aanzienlijke gevolgen. Acties van buitenlandse internetpartijen, zoals uitsluiting door browserleverancier, zullen ook aanzienlijke gevolgen hebben. Ook de vermoedelijke duur van de inbreuk van belang om te bepalen of er sprake is van aanzienlijke gevolgen. Naarmate de inbreuk langer duurt is het waarschijnlijk dat er sprake zal zijn van «aanzienlijke» gevolgen. Bij ontdekking van een inbreuk zal niet altijd direct duidelijk zijn of er sprake is van «aanzienlijke» gevolgen. Contact tussen de door inbreuk getroffen partij en de toezichthouder kan dan helpen om te bepalen of er sprake is van een meldenswaardige inbreuk. Indien daarentegen vaststaat dat een veiligheidsinbreuk of integriteitsverlies slechts beperkte impact heeft, kan een melding achterwege blijven. In het algemeen deel van de memorie van toelichting is hierop nader ingegaan (blz. 16) en is voorts ook aangegeven dat de Minister van Economische Zaken, als verantwoordelijke voor Agentschap Telecom, uit hoofde van het toezicht op de naleving van hoofdstuk 3 van de verordening door middel van bijvoorbeeld beleidsregels omstandigheden en criteria kan aanduiden waaronder een melding aan het toezichthoudend orgaan is vereist (blz. 17).

De leden van de D66-fractie vroegen zich af of er door het toezichthoudend orgaan een protocol wordt opgesteld waarmee kan worden bepaald of het publiek moet worden geïnformeerd over een veiligheidsinbreuk of integriteitsverlies. Daarnaast vroegen de leden om het «algemeen belang» te definiëren bij het informeren van het publiek. De toezichthouder zal in overleg met de door de inbreuk getroffen vertrouwensdienstverlener bepalen of en hoe het publiek moet worden geïnformeerd over een veiligheidsinbreuk of integriteitsverlies. Zo nodig zal de toezichthouder beleidsregels opstellen over het informeren van het publiek. Van het «algemeen belang» is in ieder geval sprake als gebruikers van vertrouwensdiensten door de informatie in staat worden gesteld om maatregelen te nemen die de gevolgen van de inbreuk beperken en hen duidelijkheid verschaffen over de geldigheid van transacties waarbij vertrouwensdiensten zijn gebruikt.

5.4 Uitvoeringsmaatregelen

De leden van de PvdA-fractie vroegen zich af in hoeverre de aanwijzing van de Minister van Veiligheid en Justitie als het nationale orgaan van informatieveiligheid de situatie verandert in vergelijking met de situatie tot nu toe. In de huidige situatie bevat het Besluit elektronische handtekeningen een meldplicht aan de Minister van Veiligheid en Justitie voor inbreuken op gekwalificeerde certificaten door een certificatiedienstverlener (artikel 2, onderdeel t). Die meldplicht aan de Minister heeft uitsluitend betrekking op gekwalificeerde certificaten voor elektronische handtekeningen en strekt zich niet uit tot andere gekwalificeerde vertrouwensdiensten en evenmin tot niet-gekwalificeerde vertrouwensdiensten. De in het Besluit geregelde meldplicht zal komen te vervallen gelet op de rechtstreekse werking van de verordening. In plaats daarvan bepaalt het wetsvoorstel dat de Minister van Veiligheid en Justitie het bevoegde nationale orgaan van informatieveiligheid is in de zin van de verordening. Daarmee wordt vastgelegd dat voor Nederland de Minister van Veiligheid en Justitie (ingevolge de huidige portefeuilleverdeling de Staatssecretaris) als verantwoordelijke voor het Nationaal Cyber Security Centrum het bevoegde nationale orgaan van informatieveiligheid is waaraan op grond van de verordening verleners van vertrouwensdiensten inbreuken op de veiligheid of verlies van integriteit met aanzienlijke gevolgen dienen te melden. Anders dan onder de huidige situatie heeft de aanwijzing in het wetsvoorstel daarmee tot gevolg dat een meldplicht aan de Minister van Veiligheid en Justitie zich voortaan ook tot andere soorten vertrouwensdiensten uitstrekt dan enkel gekwalificeerde certificaten voor de elektronische handtekening, waaronder voortaan ook (gekwalificeerde) certificaten voor websiteauthenticatie. Deze uitbreiding van de meldplicht bij incidenten met vertrouwensdiensten aan het NCSC zie ik, evenals melding daarvan op grond van het wetsvoorstel aan Agentschap Telecom en in voorkomend geval aan de Autoriteit persoonsgegevens (hierna ook: Ap), als een wenselijke ontwikkeling mede gelet op het incident DigiNotar in 2011.

De leden van de PvdA-fractie vroegen in hoeverre de aanwijzing van de Autoriteit persoonsgegevens als gegevensbeschermingsautoriteit de situatie verandert in vergelijking met de situatie nu. In de huidige situatie geldt op grond van artikel 34a, eerste lid, van de Wet bescherming persoonsgegevens (hierna: Wbp) een verplichting tot melding aan de Autoriteit persoonsgegevens van een inbreuk op de beveiliging als bedoeld in de Wbp, indien die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het toezicht op de naleving van deze meldplicht aan de Autoriteit persoonsgegevens berust bij deze toezichthouder. In de toekomstige situatie geldt op grond van de

verordening rechtstreeks een meldplicht voor verleners van vertrouwensdiensten aan de bevoegde nationale gegevensbeschermingsautoriteit die in de plaats komt van de in de Wbp geregelde meldplicht. Ook anders is dat de melding aan betrokkene en aan het publiek in de verordening met rechtstreekse werking is geregeld. De Europese Commissie is voorts bevoegd de bij een melding aan de bevoegde gegevensbeschermingsautoriteit over te leggen gegevens te duiden. In het wetsvoorstel wordt, voor zover de rechtstreekse werking van de verordening dit toelaat, zoveel mogelijk aangesloten bij de huidige situatie. Door aanwijzing in het wetsvoorstel van de Autoriteit persoonsgegevens als bevoegde gegevensbeschermingsautoriteit in de zin van de verordening wordt bevestigd dat een melding waarbij persoonsgegevens betrokken zijn aan deze toezichthouder dient plaats te vinden, evenals dat nu het geval is. Daarbij regelt het wetsvoorstel de mogelijkheid van handhaving door de Autoriteit persoonsgegevens. Voorts bevat het wetsvoorstel een grondslag, indien dit voor een goede uitvoering van de verordening vereist is, bij algemene maatregel van bestuur regels te stellen over de bij een melding aan de Autoriteit persoonsgegevens te verstrekken gegevens en de wijze van verstrekking daarvan. Op dezelfde wijze biedt het wetsvoorstel die grondslag voor inhoud en wijze van verstrekking voor een verplichte melding van een incident aan de Minister van Economische Zaken (AT) respectievelijk aan de Minister van Veiligheid en Justitie (NCSC). De aan Ap, AT en NCSC te melden gegevens kunnen op die wijze waar mogelijk onderling afgestemd worden vastgelegd bij algemene maatregel van bestuur. Dit is een wijziging ten opzichte van de huidige situatie. Voorts wordt anders dan in de huidige situatie in het wetsvoorstel voorzien in een verplicht op te stellen samenwerkingsprotocol tussen deze organen betreffende meldplichten, waaraan derhalve ook de Autoriteit persoonsgegevens als aangewezen bevoegde gegevensbeschermingsautoriteit deelneemt.

De leden van de D66-fractie verzochten om toelichting bij de verplichting van het samenwerkingsprotocol tussen Agentschap Telecom, de Autoriteit persoonsgegevens en het Nationaal Cyber Security Centrum. De leden vragen of de regering heeft nagedacht over het opzetten van één loket voor de meldplichten. Agentschap Telecom, de Autoriteit persoonsgegevens en het Nationaal Cyber Security Centrum hebben vanuit de verschillende rollen een belang bij de melding maar een andere taak bij de opvolging daarvan. De toezichthouders Agentschap Telecom en de Autoriteit persoonsgegevens hebben de taak om toe te zien op de naleving van de regelgeving en het NCSC heeft hulp en bijstand aan de door de inbreuk getroffen vertrouwensdienstverlener als taak. Het samenwerkingsprotocol borgt dat toezichthouders en het NCSC bij de melding en opvolging daarvan samen optrekken. In een dergelijk protocol kunnen ook afspraken worden opgenomen over de initiële melding, bijvoorbeeld via een bepaald loket. Op deze wijze kan eenmalige aanlevering en meervoudig gebruik van meldingsgegevens worden gerealiseerd, waardoor de administratieve lasten van de melding beperkt blijven. Verder borgt het samenwerkingsprotocol dat bij de opvolging van melding niet langs elkaar heen wordt gewerkt. Bij de vervolgacties zullen de toezichthouders en het NCSC in onderlinge afstemming op grond van hun eigen taken en bevoegdheden opereren. Voor het NCSC is bij meldingen van belang om voor vertrouwensdienstverleners een veilig klimaat te creëren waarin deze bereid zijn om incidenten te melden aan het NCSC, zodat indien nodig hulp en bijstand kan worden verleend.

De leden van de D66-fractie vroegen of door middel van een tabel een overzicht gegeven kan worden van de verschillende types meldplichten. Hieronder is een tabel afgebeeld met meldplichten die op het verlenen van vertrouwensdiensten betrekking hebben.

	Huidige meldplicht	Toekomstige meldplicht
ACM	gekwalificeerde certificaten voor elektronische handtekening	niet van toepassing
AT	niet van toepassing	gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten
NCSC	gekwalificeerde certificaten voor elektronische handtekening	gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten[1]
Ap	ongeacht aard van de activiteit, indien inbreuk of verlies (ook) persoonsgegevens betreft	ongeacht aard van de activiteit, indien inbreuk of verlies (ook) persoonsgegevens betreft

[1] Naast de verordening en ter uitvoering daarvan dit wetsvoorstel, bevat ook het wetsvoorstel Wet gegevensverwerking en meldplicht cybersecurity (Kamerstukken 34 388) een voor vertrouwensdiensten relevante meldplicht aan de Minister van Veiligheid en Justitie (NCSC). In hoeverre en op welke wijze aanbieders van vertrouwensdiensten onder het toepassingsbereik van ook dat wetsvoorstel zullen vallen is afhankelijk van de vraag in hoeverre deze aanbieders als aanbieders van vitale diensten moeten worden aangemerkt. Vertrouwensdiensten maken deel uit van een onderzoek dat loopt naar de herijking van diensten die vitaal zijn in de Nederlandse Telecomsector.

In deze tabel zijn geen situaties verwerkt waarbij een aanbieder (ook) in een andere hoedanigheid dan als verlener van vertrouwensdiensten optreedt, bijvoorbeeld als aanbieder van een openbare telecommunicatiedienst. Het is telkens afhankelijk van de aard van de activiteit en de aard van de inbreuk of, aan wie en in hoeverre meldplichten aan de orde zijn. Ook loopt bovenstaande tabel niet vooruit op toekomstige of bestaande nog te implementeren of uit te voeren Europese regelgeving.

De leden van de D66-fractie vroegen of de regering heeft nagedacht over het opzetten van één loket voor de meldplichten. In antwoord op een eerdere vraag van deze leden in deze paragraaf over het samenwerkingsprotocol is hier op ingegaan, zodat hier wordt volstaan door naar dat antwoord te verwijzen.

5.5 Gekwalificeerde vertrouwensdiensten en vertrouwenslijsten

De leden van de PvdA-fractie geven aan dat er ook een meldplicht geldt op grond van de verordening aan het toezichthoudend orgaan bij integriteitsverlies met aanzienlijke gevolgen en vragen zich af wat in dit geval onder «aanzienlijke gevolgen» wordt verstaan en welke instantie dit begrip nader gaat invullen. De begrenzing in de verordening van de plicht tot melden bij een integriteitsverlies met aanzienlijke gevolgen geldt ook voor de plicht tot melden van een veiligheidsinbreuk. Op de nadere invulling van het begrip «aanzienlijke gevolgen» is in antwoord op een soortgelijke vraag in paragraaf 5.3 van de leden van de D66-fractie ingegaan. Hier wordt naar dat antwoord verwezen.

De leden van de PvdA-fractie vroegen welke instantie het begrip «aanzienlijk gevolgen» nader gaat invullen. Daarnaast verzochten deze leden of dit leidt tot overplaatsing van personeel van de Autoriteit Consument en Markt naar Agentschap Telecom. In antwoord op een eerdere vraag van de leden van de D66-fractie in paragraaf 5.3 is nader ingegaan op het begrip aanzienlijke gevolgen. Het begrip zal door de toezichthouder Agentschap Telecom in samenspraak met de geëigende Europese instanties zoals ENISA (European Union Agency for Network and Information Security) en FESA (Forum of European Supervisory Authorities) nader worden ingevuld. Hierbij wordt nog onderzocht of hiervoor beleidsregels zullen worden vastgesteld. Er is geen sprake van overplaatsing van personeel van ACM naar AT. Verschillende medewerkers hebben uit eigen beweging een overstap gemaakt van ACM naar AT waarmee belangrijke kennis voor de toezichttaak behouden blijft.

De leden van de PVV-fractie waren benieuwd of het toezichthoudend orgaan in Nederland gekwalificeerde dienstverleners uit andere EU-lidstaten met een vertrouwensmerk van de Europese Unie nog op enigerlei wijze controleert dan wel dat die automatisch op de vertrouwenslijst van iedere lidstaat moeten worden opgenomen. Indien een vertrouwensdienstverlener in een andere lidstaat van de Europese Unie is gevestigd, is het door die andere lidstaat aangewezen toezichthoudend orgaan verantwoordelijk voor de beoordeling van de toekenning van de status gekwalificeerd aan die dienstverlener en de door hem verleende vertrouwensdienst met inachtneming van het daaromtrent in de verordening bepaalde. Indien de status gekwalificeerd is toegekend en na registratie op de vertrouwenslijst is geplaatst door het desbetreffende toezichthoudend orgaan, mag de gekwalificeerde vertrouwensdienstverlener het vertrouwensmerk van de Europese Unie gebruiken voor de gekwalificeerde vertrouwensdienst die hij levert. Voor de duur dat een vertrouwensdienstverlener over de status gekwalificeerd beschikt is het toezichthoudend orgaan uit de andere lidstaat verantwoordelijk voor het toezicht op de naleving van de aan die status verbonden eisen in de verordening. Ingeval op grond van de verordening aan het toezichthoudend orgaan een inbreuk op de veiligheid of integriteit is gemeld die ook Nederland treft, stelt dat toezichthoudende orgaan het Nederlandse toezichthoudende orgaan en Enisa («European Union Agency for Network and Information Security») daarvan op de hoogte en kan het om bijstand aan het Nederlandse toezichthoudende orgaan verzoeken.

5.6 Uitvoeringsmaatregelen

De leden van de PvdA-fractie vroegen of er in 2011 bij DigiNotar sprake was van een veiligheidsinbreuk en integriteitsverlies met aanzienlijke gevolgen. Deze leden vroegen verder of dit toen ook binnen 24 uur gemeld is aan een toezichthoudend orgaan. Tot slot vroegen deze leden zich af of de afwikkeling van het DigiNotarlek met dit wetsvoorstel op een andere manier zou gebeuren dan tot nu toe.
Bij de DigiNotarzaak was er inderdaad sprake van een veiligheidsinbreuk en integriteitsverlies met aanzienlijke gevolgen. Het incident bij Diginotar leidde tot gebruik van de rijkscrisisstructuur waaraan een veelheid aan organisaties en het bedrijfsleven hebben deelgenomen om de zorgen omtrent uitval van essentiële digitale datacommunicatie weg te nemen. Het betrof gecompromitteerde Public Key Infrastructure (PKI)-certificaten van het bedrijf DigiNotar die de gebruikers van onder meer (overheids-)sites moest garanderen dat zij daadwerkelijk op de site van hun keuze kwamen. Door het onbruikbaar worden van de certificaten werd een essentieel onderdeel van betrouwbare digitale informatievoorziening aangetast en konden in potentie ernstige verstoringen optreden. Een beschrijving van de ontwikkeling van deze crisis is terug te vinden in de Evaluatie van de Rijkscrisisorganisatie tijdens de DigiNotar-crisis door de Inspectie Veiligheid en Justitie (bijlage bij Kamerstukken II 2011/12, 26 643, nr. 250). Het incident leidde tot het ongeldig worden van alle door DigiNotar uitgegeven certificaten waardoor de vertrouwensdiensten niet meer bruikbaar waren en moesten worden vervangen. De inbreuk is destijds niet binnen 24 uur gemeld aan het toezichthoudend orgaan. Een verplichting hiertoe staat anders dan indertijd nu duidelijk in de verordening vermeld.
Indien de verordening en dit wetsvoorstel als in werking getreden wet indertijd er al waren en door de getroffen partij in acht waren genomen, is het goed denkbaar te veronderstellen dat de afwikkeling van het incident anders was gelopen dan destijds. Met melding van een veiligheidsinbreuk of integriteitsverlies is eerder hulp en bijstand van het NCSC mogelijk waardoor de gevolgen van een inbreuk beperkt kunnen worden. De verordening regelt vroegtijdige betrokkenheid van toezichthouders en het

NCSC. Daarnaast is communicatie aan het publiek belangrijk waardoor aan herstel van geschaad vertrouwen kan worden gewerkt.

De leden van de PvdA-fractie verzochten onder verwijzing naar het schrappen van artikel 18.7 van de Telecommunicatiewet de verschillen en overeenkomsten tussen Nederlandse en Europese eisen aan te geven die aan certificatiedienstverleners worden gesteld. De vooral organisatorische eisen waaraan een certificatiedienstverlener dient te voldoen die certificaten als gekwalificeerde certificaten aanbiedt of afgeeft aan het publiek en in Nederland een vestiging heeft, zijn niet onderwerp van het huidige artikel 18.7 maar van het huidige artikel 18.15, eerste lid, van de Telecommunicatiewet. Daarin is bepaald dat certificatiedienstverleners dienen te voldoen aan de eisen gesteld bij of krachtens algemene maatregel van bestuur. Deze eisen zijn in artikel 2 van het Besluit elektronische handtekeningen vastgesteld en zullen vervallen doordat artikel 24 van de verordening zelf voorziet in eisen waaraan gekwalificeerde verleners van vertrouwensdiensten moeten voldoen. De eisen uit het besluit worden niet allemaal geheel letterlijk gedekt door de eisen uit de verordening:

– In het besluit wordt bijvoorbeeld een verklaring van een daartoe bevoegde instantie geëist waaruit blijkt dat, kort gezegd, bestuurders en medewerkers van de certificatiedienstverlener in de laatste vier jaar niet voor een misdrijf onherroepelijk zijn veroordeeld. De eidas-verordening bepaalt uitsluitend dat »betrouwbaar» personeel in dienst genomen moet worden. In het kader van toezicht en de daarbij behorende beoordeling van conformiteitsbeoordelingsverslagen zal de invulling hiervan in de praktijk nadere invulling dienen te krijgen;
– Het besluit vereist procedures en processen op het gebied van administratie en beheer overeenkomstig een beschreven kwaliteitssysteem dat in overeenstemming is met de laatste ontwikkelingen op het gebied van kwaliteitssystemen. Dit is een concretisering van de eis uit de verordening die voorschrijft dat de gekwalificeerde verlener van vertrouwensdiensten administratieve en managementprocedures toepast die voldoen aan Europese of internationale normen;
– Het besluit bevat eisen met betrekking tot de verplichte inhoud van een beëindigingsplan. Deze eisen bleken in praktijk slecht werkbaar. Een nadere invulling van het beëindigingsplan, is afhankelijk van de praktijk;
– Het besluit vereist de beschikking over en het hanteren van beschreven klachtenafhandeling- en geschillenbeslechtingprocedures; dit is een concretisering van de eis uit de verordening die voorschrijft dat de gekwalificeerde verlener van vertrouwensdiensten administratieve en managementprocedures toepast die voldoen aan Europese of internationale normen.
– Het informeren over het bestaan van vrijwillige accreditatie; met het schrappen van het wettelijk vermoeden van overeenstemming en het vervallen van het TTP.NL schema is deze eis niet meer van toepassing;
– Het besluit verplicht tot het opnemen van eventuele beperkingen betreffende het gebruik of de hoogte van de transactiewaarde van het gekwalificeerde certificaat in dat certificaat. Op deze bepaling werd zelden een beroep gedaan. Het opnemen van beperkingen is nog steeds mogelijk, maar dat hoeft niet in het gekwalificeerde certificaat te worden gedaan.

5.7 Toezicht en handhaving

De leden van de CDA-fractie informeerden hoe in Nederland de verplichting wordt ingericht om voorschriften vast te stellen inzake sancties die doeltreffend, evenredig en afschrikkend dienen te zijn. In artikel 15.1, eerste lid, van de Telecommunicatiewet zijn de onderwerpen

vastgesteld waarvoor de bij besluit van de Minister van Economische Zaken aangewezen ambtenaren zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens die wet daarover. Dit betreft het toezicht dat door Agentschap Telecom wordt uitgeoefend. In de in onderdeel I van het wetsvoorstel voorgestelde wijziging van artikel 15.1, aanhef en eerste lid, strekt dit toezicht door AT zich voortaan ook uit tot het verlenen van vertrouwensdiensten door in Nederland gevestigde verleners van vertrouwensdiensten als geregeld in de voor deze diensten relevante delen van de verordening en tot enkele andere in het wetsvoorstel geregelde zaken. Het gevolg van deze taakuitbreiding van AT is dat de daarmee belaste ambtenaren van AT hiervoor toezichthouder zijn als bedoeld in artikel 5:11 van de Awb en bevoegdheden tot handhaving beschikbaar zijn die ook voor andere toezichtstaken in de Tw geregeld zijn, zoals de toepassing van bestuursdwang (artikel 15.2, van de Tw) en het door de Minister opleggen van een bestuurlijke boete (artikel 15.4, van de Tw). Daarmee is het reguliere regime van de Tw voor toezicht onder verantwoordelijkheid van de Minister met de daarbij behorende sancties tot handhaving van toepassing. Daarnaast volgt uit het voorgestelde nieuwe artikel 15.1, tweede lid, dat de bij besluit van de Autoriteit persoonsgegevens aangewezen ambtenaren belast zijn met het toezicht op de naleving van de in de verordening geregelde meldplicht voor een veiligheidsinbreuk die of verlies van integriteit dat aanzienlijke gevolgen heeft voor persoonsgegevens. Dit toezicht op de naleving strekt zich voorts ook uit tot de bij een melding te overleggen gegevens. Met deze voorgestelde uitbreiding in de Telecommunicatiewet van het toezicht en handhaving door Ap, ontstaat ook de bevoegdheid voor Ap de in die wet reeds geregelde mogelijkheden van sancties inzake last onder bestuursdwang en bestuurlijke boete toe te passen (artikelen 15.2 en 15.4).

De leden van de CDA-fractie vragen zich af hoe de regering zich voorstelt dat aanbieders van vertrouwensdiensten een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de verleende vertrouwensdienst, of voor de persoonsgegevens die daarmee worden beheerd, binnen 24 uur na ontwikkeling moeten melden. Daarbij verzoeken deze leden hoe de regering dit concreet wil gaan uitwerken en of dit uitvoerbaar is. Het voorschrift op basis waarvan voortaan gemeld dient te worden is in artikel 19, tweede lid, van de verordening vastgelegd. Voor vertrouwensdienstverleners is van belang dat dit voorschrift voor hen voldoende duidelijk is om te kunnen naleven. Naarmate voor hen meer houvast bestaat om dit voorschrift goed te kunnen naleven, gaat hier ook een grotere werking vanuit. In antwoord op een eerdere vraag van de leden van de PvdA-fractie onder paragraaf 5.5 is aangegeven dat door middel van bijvoorbeeld beleidsregels de Minister van Economische Zaken (AT) omstandigheden en criteria kan aanduiden waaronder een melding aan het toezichthoudend orgaan is vereist. In de huidige situatie gelden voorts al meldplichten voor gekwalificeerde certificatiedienstverleners voor elektronische handtekeningen. Bij deze certificatiedienstverleners is eerder al actief het belang onder de aandacht gebracht om beveiligingsincidenten te melden; die boodschap kan bijvoorbeeld worden herhaald tijdens bedrijfsbezoeken door Agentschap Telecom. Ook communicatie via de eigen website van Agentschap Telecom kan de aandacht hiervoor versterken, zoals voor verleners van niet-gekwalificeerde vertrouwensdiensten. Voorts vervullen NCSC en AP in de kenbaarheid van de meldplicht vanuit hun eigen verantwoordelijkheid eveneens een rol. Voor de uitvoerbaarheid is tevens van belang dat de bij een melding te verstrekken gegevens aan AT, NCSC en in voorkomend geval ook aan AP voldoende samenhangend zijn vastgesteld. Het wetsvoorstel voorziet in een grondslag om die gegevens voor alle drie de organen bij algemene maatregel van bestuur vast te stellen, indien dit voor de goede uitvoering van de verordening vereist is. Voorts bevat het

wetsvoorstel de verplichting tot het sluiten van een samenwerkingsprotocol tussen AT, NCSC en AP. Hierover zijn inmiddels gesprekken gaande. Een dergelijk protocol kan bijvoorbeeld betrekking hebben over de wijze waarop een melding dient plaats te vinden, bijvoorbeeld via een bepaald loket. Of afspraken bevatten over het gecoördineerd organiseren van overleg met een betrokken dienstverlener naar aanleiding van een melding en het daarop volgende toezicht. Langs deze lijnen wordt de uitvoering van de meldplicht nader ingericht.

Voorts verzochten de leden van de CDA-fractie ook specifiek in te gaan op de handhaving van de meldplichten uit de verordening, en of er sancties gelden bij niet-tijdige melding, en zo ja, welke. Het wetsvoorstel voorziet in mogelijkheden tot handhaving van de meldplichten uit de verordening door Agentschap Telecom en door de Autoriteit persoonsgegevens. In antwoord op een eerdere vraag van de leden van de CDA-fractie in deze paragraaf over het kunnen opleggen van sancties door het toezichthoudend orgaan, is toegelicht dat de reguliere bevoegdheden waarover Agentschap Telecom op grond van de Telecommunicatiewet als toezichthouder tot handhaving beschikt zich ingevolge het wetsvoorstel uitstrekken tot een geheel aan verplichtingen in de verordening. Deze verplichtingen in de verordening waarop dat toezicht betrekking heeft, omvatten ook de daarin vastgelegde meldplichten aan het toezichthoudend orgaan. Agentschap Telecom is daardoor als toezichthouder bevoegd naar aanleiding van een melding verdere informatie in te winnen en indien nodig handhavend optreden, zoals door middel van oplegging van een last onder bestuursdwang, last onder dwangsom ingevolge afdeling 5.3.2 van de Awb, of het opleggen van een bestuurlijke boete. Deze laatste bevoegdheid kan daarmee in het kader van handhaving bij een niet tijdige melding van een incident zo nodig worden toegepast. Het wetsvoorstel bepaalt voorts dat de bij besluit van de Autoriteit persoonsgegevens aangewezen ambtenaren belast zijn met het toezicht op de naleving van onder meer de meldplicht in de verordening voor zover het persoonsgegevens betreft. Met deze voorgestelde uitbreiding in de Telecommunicatiewet van het toezicht en handhaving door Ap, beschikt Ap over de in die wet reeds geregelde mogelijkheden tot handhaving zoals ook Agentschap Telecom daarover beschikt (artikelen 15.2 en 15.4 van de Telecommunicatiewet). De verplichte melding aan NCSC is niet onderworpen aan toezicht en handhaving. Dit sluit aan bij de huidige wijze waarop een meldplicht voor certificatiedienstverleners in het Besluit elektronische handtekeningen is geregeld.

De leden van de CDA-fractie vroegen of het klopt dat het toezicht en de handhaving op gekwalificeerde certificaten voor elektronische handtekeningen wordt weggehaald bij de ACM en waarom. Het wetsvoorstel regelt de overgang van het toezicht van ACM naar AT. ACM is een markttoezichthouder waarbij de voor het toezicht op de verordening benodigde technische expertise te beperkt voorhanden is. Het toezicht op vertrouwensdiensten sluit daarbij niet aan op de overige taken van ACM. De benodigde technische expertise is wel voorhanden bij Agentschap Telecom dat meer technisch inhoudelijk toezicht op complexe materie uitvoert. Het toezicht op de verordening past daar goed bij. Bij het toezicht op de verordening zal, meer dan onder uit de huidige wet inhoudelijk technisch toezicht op de eisen van de verordening nodig zijn. De gemaakte afwegingen betreffende de veranderingen in toezicht en de verplaatsing daarvan zijn in paragraaf 5.8 van de memorie van toelichting nader toegelicht. Tot de inwerkingtreding van het wetsvoorstel zal het toezicht nog door ACM worden uitgevoerd. Daarbij maakt ACM gebruik van personeel van AT indien het wetsvoorstel later dan 1 juli 2016 tot wet wordt verheven en in werking treedt. Hierover worden afspraken gemaakt.

De vertrouwensdienstverleners worden geïnformeerd over het toezicht in deze tijdelijke situatie.

5.8 Uitvoeringsmaatregelen

De leden van de VVD-fractie vroegen in hoeverre het instrument «audit» door de conformiteitsbeoordelingsinstantie als ondersteuning van de naleving voldoende is uitgewerkt en vroegen daarop een toelichting. Deze leden vroegen voorts of de regering op de hoogte is van de bevindingen van de parlementaire enquête Fyra ten aanzien van de definiëring van het begrip audit. Om de waarde die aan een audit kan worden toegekend te bepalen is van belang om te weten wat er wordt gecontroleerd en of de gehanteerde normen voldoende houvast bieden om vast te stellen of aan de regels is voldaan. De verordening geeft aan dat het doel van de audit is te bevestigen dat gekwalificeerde verleners van vertrouwensdiensten en de gekwalificeerde vertrouwensdiensten die door hen worden verleend, voldoen aan de in de verordening vastgestelde eisen. Mede door de komst van de verordening zijn de normen voor gekwalificeerde verleners van vertrouwensdiensten verder uitgewerkt en expliciet gemaakt. Er zijn verschillende wijze van auditen. Een les die uit de DigiNotarzaak is geleerd, is dat een zogeheten managementaudit, waarbij het in staat zijn om aan de regels te voldoen centraal staat, niet langer voldoende is om een hoge mate van betrouwbaarheid te garanderen. Bij de audit zal de technische betrouwbaarheid en veiligheid bij de vertrouwensdienstverlener en de verleende vertrouwensdiensten zelf meer centraal komen te staan. In audittermen heet dit een productcertificatie. Voor de conformiteitsbeoordelingsinstantie betekent dit dat deze ook aan andere eisen moet voldoen dan voorheen. Het voldoen aan deze eisen wordt getoetst bij de accreditatie waartoe de verordening de conformiteitsbeoordelingsinstantie verplicht. Bij de accreditatie wordt ook beoordeeld of de gehanteerde normen een goede uitwerking zijn om het doel van de audit, namelijk het voldoen aan de in de verordening gestelde eisen, te borgen. In de reactie op de parlementaire enquête Fyra zal door de regering worden ingegaan op de lessen die daaruit worden getrokken.
De leden van de PvdA-fractie vroegen waarom artikel 18.16a van de Telecommunicatiewet over het vermoeden van overeenstemming vervalt. Het vermoeden van overeenstemming vervalt om de toezichthouder een stevigere rol te geven bij het toezicht op de vertrouwensdienstverlener. Hiermee wordt een aanbeveling van de Onderzoeksraad voor Veiligheid opgevolgd. Het vermoeden van overeenstemming verplichtte de toezichthouder tot het toekennen van het vermoeden dat aan de regels van de Wet elektronische handtekeningen was voldaan als een aanbieder beschikte over een zogeheten TTP-verklaring. De toezichthouder had dan nauwelijks ruimte meer om zelf onderzoek te doen en zich een oordeel te vormen over de naleving van de regels door de aanbieder. Dit is onwenselijk en door het schrappen van het vermoeden van overeenstemming is de rol en verantwoordelijkheid van de toezichthouder aangepast en vergroot. Een conformiteitsbeoordelingsrapport vormt een belangrijk onderdeel, maar het eindoordeel over het al dan niet voldoen aan de wettelijke eisen van de verordening is aan de toezichthouder.

De leden van de D66 fractie vroegen of het wenselijk is om een Europees conformiteitbeoordelingsschema te laten ontwikkelen zonder het gebruik hiervan te verplichten. Deze leden wilden graag weten of een dergelijk schema wordt ontwikkeld en wat de voortgang daarvan is. Tot slot verzochten deze leden meer uit te leggen waarom een wettelijke verplichting van een Europees conformiteitsbeoordelingsschema niet wenselijk is. Het ontbreken van een Europees conformiteitbeoordelingsschema zal leiden tot verschillen tussen de conformiteitsbeoordelingen en -verslagen tussen de lidstaten. Vanwege de verplichte grensoverschrij-

dende erkenning van vertrouwensdiensten is harmonisatie van conformiteitbeoordelingen en -verslagen wenselijk, zodat toezichthouders in andere lidstaten kunnen weten wat er is getoetst en wat hiervan het resultaat was. De European co-operation for Accreditation (EA) is voornemens om een Europees conformiteitbeoordelingsschema te ontwikkelen. Deze ontwikkeling bevindt zich thans in de beginfase. Het wettelijk verplicht stellen van het gebruik van een eventueel Europees auditschema betekent dat de wijze waarop een conformiteitsbeoordelingsinstantie een beoordeling dient uit te voeren specifiek en met uitsluiting van andere schema's wettelijk is voorgeschreven. Dit roept de vraag op of gebruik van het schema niet ook tot enig wettelijk vermoeden leidt dat aan de eisen in de verordening is voldaan zodra een conformiteitsbeoordelingsinstantie dit wettelijk voorgeschreven schema aanhoudt. Indien dit laatste in de wet zou worden bevestigd, belemmert dat evenwel de mogelijkheden voor het daadwerkelijk uitoefenen van toezicht door de toezichthouder. In feite wordt dan teruggekeerd naar een situatie in de wet die gelijkenis heeft met de huidige situatie waarin met een wettelijk vermoeden van overeenstemming wordt gewerkt op basis van een beoordeling door een gecertificeerde instelling. Dit is niet wenselijk gelet op de aanbeveling om de rol van de toezichthouder aan te passen, zoals door de Onderzoeksraad voor Veiligheid in zijn onderzoeksrapport naar aanleiding van het incident met DigiNotar is aangegeven. Ook het wettelijk voorschrijven van een Europees schema zonder dat daaraan een enkel wettelijk vermoeden van overeenstemming mag worden ontleend, leidt tot een situatie waarin de toezichthouder minder ruimte heeft om zo nodig afstand te nemen van een beoordelingsverslag of bij het volgen van dat schema zo nodig eigen accenten of kanttekeningen te plaatsen op specifieke onderdelen daarvan. Dit geldt dan ook voor een eventueel door een conformiteitsbeoordelingsinstantie gevolgd Europees schema. Gelet hierop is er vanaf gezien in het wetsvoorstel een schema aan te wijzen.

5.9 Aansprakelijkheid

De leden van de PvdA-fractie vroegen of het juist was dat voor gekwalificeerde verleners van vertrouwensdiensten een omkering van de bewijslast geldt en hoe dit zich verhoudt tot de omkering van de bewijslast (het rechtsvermoeden) uit de Mijnbouwwet. De verordening regelt een wettelijk bewijsvermoeden dat ziet op de aansprakelijkheid van gekwalificeerde verleners van vertrouwensdiensten. Verleners van vertrouwensdiensten zijn aansprakelijk voor opzettelijk of uit onachtzaamheid toegebrachte schade door het niet naleven van de verordening. Indien het gaat om een gekwalificeerde verlener van vertrouwensdiensten, wordt de opzet of nalatigheid bij het zich voordoen van schade vermoed aanwezig te zijn, behoudens tegenbewijs. Het vermoeden geldt dus ten aanzien van de opzet of nalatigheid van de gekwalificeerde verlener van vertrouwensdiensten. Het wetsvoorstel bewijsvermoeden gaswinning Groningen regelt eveneens een wettelijk bewijsvermoeden. Dat bewijsvermoeden heeft betrekking op schade door de gaswinning uit het Groningenveld en ziet op de aansprakelijkheid van de mijnbouwexploitant. Voor mijnbouwexploitanten geldt een risicoaansprakelijkheid. Dat wil zeggen dat, anders dan bij gekwalificeerde verleners van vertrouwensdiensten, opzet of nalatigheid geen vereiste is voor aansprakelijkheid. Het bewijsvermoeden met betrekking tot mijnbouwactiviteiten geldt dan ook niet ten aanzien van de opzet of nalatigheid van de exploitant, maar ten aanzien van de oorzaak van de schade. Indien sprake is van fysieke schade aan gebouwen en werken binnen het effectgebied van het Groningenveld, die naar haar aard schade als gevolg van bodembeweging door de gaswinning zou kunnen zijn, wordt vermoed dat de schade het gevolg is van de gaswinning. Omdat mijnbouwexploitanten

geen gekwalificeerde verleners van vertrouwensdiensten zijn, is er geen relatie tussen de beide bewijsvermoedens.

De leden van de PVV-fractie vragen waarom voor een constructie is gekozen waarbij niet-gekwalificeerde vertrouwensdienstverleners niet de bewijslast dragen voor schade toegebracht aan een persoon vanwege het niet naleven van de verplichtingen uit de verordening, terwijl dit voor gekwalificeerde verleners wel het geval is. De verordening vervangt richtlijn 1999/93/EG van het Europees parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG 2000, L 13). In deze richtlijn is voorzien in een aansprakelijkheidsregeling voor de gekwalificeerde verlener van vertrouwensdiensten die inhoudt dat deze aansprakelijk is voor schade die als gevolg van bepaalde omstandigheden is geleden door personen die in redelijkheid op het certificaat hebben vertrouwd. Als de gekwalificeerde vertrouwensdienstverlener kan aantonen dat hij niet onzorgvuldig heeft gehandeld, is hij van zijn aansprakelijkheid ontheven. Voor certificatiedienstverleners die andere, niet-gekwalificeerde, certificaten afgaven geldt deze regeling niet. Deze zijn onderworpen aan de nationale aansprakelijkheidsregels. In de verordening is eveneens onderscheid gemaakt tussen gekwalificeerde en niet-gekwalificeerde verleners van vertrouwensdiensten. Hoewel de overwegingen in de verordening zich daarover niet uitdrukkelijk uitlaten is de achtergrond van dit onderscheid vermoedelijk daarin gelegen dat eerder gerechtvaardigd op gekwalificeerde vertrouwensdienstverleners en hun certificaten mag worden vertrouwd dan op niet-gekwalificeerde vertrouwensdienstverleners en hun diensten. Op gekwalificeerde vertrouwensdienstverleners en gekwalificeerde vertrouwensdiensten zijn in de verordening meer en specifiekere eisen, conformiteitsbeoordelingen en toezicht voor- en achteraf van toepassing. Deze maatregelen leiden tot het gerechtvaardigd mogen vertrouwen op deze gekwalificeerde verleners van vertrouwensdiensten. Dit is op het punt van de aansprakelijkheid uitgewerkt in de vorm van een bewijsvermoeden.

De leden van de PVV-fractie vroegen of ook bij niet-gekwalificeerde verleners van vertrouwensdiensten de bewijslast kan worden gelegd. Het antwoord luidt ontkennend. De verordening bepaalt in artikel 13, eerste lid, tweede volzin dwingend dat de bewijslast voor het aantonen van opzet of nalatigheid van een niet-gekwalificeerde verlener van vertrouwensdiensten ligt bij de natuurlijke persoon of de rechtspersoon die zich op de schade beroept, die is te wijten aan een verzuim in de niet-naleving van de verplichtingen in de verordening.

De leden van de PVV-fractie vroegen hoe een Nederlandse burger kan controleren of een verlener van vertrouwensdiensten gekwalificeerd is of niet. Hiervoor kan de vertrouwenslijst worden geraadpleegd waarvoor ingevolge de verordening het toezichthoudend orgaan verantwoordelijk voor is. Doel van de vertrouwenslijst is dat bij gebruik van gekwalificeerde vertrouwensdiensten de ontvangende partij in staat is om gekwalificeerde vertrouwensdiensten op betrouwbaarheid te beoordelen. De vertrouwenslijst bevat daartoe informatie over de uitgever van de digitale gekwalificeerde certificaten en andere informatie over de vertrouwensdienst. Thans is de Autoriteit Consument en Markt verantwoordelijk voor het bijhouden van de vertrouwenslijst. Op de website van ACM is de vertrouwenslijst te raadplegen. Naast een menselijk leesbare versie is er ook een machinaal verwerkbare versie van de vertrouwenslijst.

De leden van de D66-fractie wezen op de mogelijkheid dat verleners van vertrouwensdiensten, onder bepaalde voorwaarden, beperkingen verbinden aan het gebruik van de door hen verleende diensten en dat zij

niet aansprakelijk zijn voor schade die het gevolg is van het gebruik dat deze beperkingen te buiten gaat. Zij vroegen aan te geven onder welke specifieke voorwaarden dergelijke beperkingen verbonden kunnen worden aan verleende diensten. Ingevolge artikel 13, tweede lid, van de verordening gelden twee voorwaarden voor het niet aansprakelijk zijn voor schade die ontstaat door gebruikmaking van diensten die de aangegeven beperkingen overschrijden. De eerste voorwaarde is dat klanten vooraf goed worden geïnformeerd over de beperkingen. De tweede voorwaarde is dat beperkingen herkenbaar moeten zijn voor een derde partij. Van dit laatste kan, zoals in overweging 37 is aangegeven, sprake zijn doordat informatie over de beperkingen wordt opgenomen in de voorwaarden met betrekking tot de verleende dienst, of via andere herkenbare middelen.

Deze leden vroegen voorts wanneer er sprake is van het «terdege» informeren van klanten. In overweging 37 van de verordening wordt van «terdege» informeren gesproken en in de verordening wordt in artikel 13, tweede lid, de terminologie «goed» informeren gebruikt. Deze wijze van informeren zal in redelijkheid betekenen dat klanten van juiste en voldoende informatie worden voorzien, zodat voor hen duidelijk is waar de beperkingen van het gebruik betrekking op hebben.
De leden van de PvdA-fractie vroegen naar de verschillen en overeenkomsten tussen de Nederlandse regels (art. 6:196b BW) en de Europese regels (artikel 13 van de verordening) met betrekking tot de aansprakelijkheid van certificatiedienstverleners.
Het ter implementatie van de Richtlijn elektronische handtekeningen opgenomen artikel 6:196b BW betreft de aansprakelijkheid van certificatiedienstverleners die gekwalificeerde certificaten afgegeven aan het publiek of voor een zodanig certificaat instaan, voor schade die door personen die in redelijkheid op dit certificaat hebben vertrouwd, is geleden. De schade dient te zijn geleden als gevolg van de in het artikel 196b lid 2 genoemde omstandigheden. De certificatiedienstverlener is op grond van het tweede lid aansprakelijk voor de:
– de juistheid, op het tijdstip van afgifte, van alle gegevens in het gekwalificeerde certificaat en de opneming van alle voor dit certificaat voorgeschreven gegevens;
– de garantie dat de in het gekwalificeerd certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het certificaat, houder was van de gegevens voor het aanmaken van de handtekening, die met de in het certificaat gegeven of geïdentificeerde gegevens voor het verifiëren van een handtekening overeenstemmen;
– de garantie dat de gegevens voor het aanmaken van de handtekening en die voor het verifiëren van de handtekening, – ingeval zij beide door de certificatiedienstverlener werden gegenereerd –, complementair kunnen worden gebruikt;
– het niet registreren van de intrekking van het certificaat.
Indien de desbetreffende certificatiedienstverlener aan kan tonen dat hij niet onzorgvuldig heeft gehandeld, is hij van zijn aansprakelijkheid ontheven.
Voor dienstverleners van niet-gekwalificeerde certificaten gelden thans de nationale aansprakelijkheidsregels (het algemene aansprakelijkheidsregime van Boek 6 BW).
Artikel 13 van de verordening regelt de aansprakelijkheid van zowel gekwalificeerde als niet gekwalificeerde verleners van vertrouwensdiensten.
Ingevolge artikel 13 zijn niet-gekwalificeerde verleners van vertrouwensdiensten aansprakelijk voor opzettelijk of uit onachtzaamheid toegebrachte schade aan een natuurlijke persoon of rechtspersoon die is te wijten aan een verzuim de verplichtingen uit hoofde van de verordening na te leven. De bewijslast hiervoor ligt bij de natuurlijke persoon of de

rechtspersoon. Voor verleners van gekwalificeerde verleners van vertrouwensdiensten geldt dat de opzet of nalatigheid van een gekwalificeerde verlener van vertrouwensdiensten wordt vermoed (bewijsvermoeden), tenzij die bewijst dat de schade zonder opzet of nalatigheid van zijn kant is ontstaan. De bewijslast ligt op dit punt bij de gekwalificeerde verlener van vertrouwensdiensten.

5.10 Uitvoeringsmaatregelen

5.11 Derde landen

De leden van de PvdA-fractie verzochten of er op dit moment al veel overeenkomsten van de EU en derde landen over erkenning van certificaten zijn. Deze leden vroegen hoeveel van dergelijke overeenkomsten worden voorzien. De Richtlijn elektronische handtekeningen bood derde landen reeds de mogelijkheid tot het afsluiten van overeenkomsten met de EU. Hiervan is in de praktijk tot op heden geen gebruik gemaakt. Gelet op deze ervaring, is de verwachting dat het aantal derde landen dat een overeenkomst met de Europese Unie wil afsluiten voorlopig beperkt zal blijven.

5.13 Toegankelijkheid voor personen met een handicap

De leden van de SP-fractie waren benieuwd naar de criteria voor toegankelijkheid van vertrouwensdiensten voor personen met een handicap. Deze leden vroegen op welke wijze vertrouwensdiensten voor gehandicapten worden onderscheiden van anderen. Tot slot verzochten deze leden welke belemmeringen er bestaan om deze toegankelijkheid verplicht te stellen. De verordening bevat geen criteria voor toegankelijkheid voor personen met een handicap. Wanneer mensen met een handicap kunnen werken met een computer levert het gebruik van vertrouwensdiensten doorgaans geen problemen op. In situaties dat personen met een handicap stuiten op toegankelijkheidsproblemen kunnen de vertrouwensdienstverleners helpen bij het zoeken naar een oplossing. Zo is het voor visueel gehandicapten niet mogelijk om codes te lezen die nodig zijn voor het gebruik van een vertrouwensdienst. Een oplossing is dan software waarmee de codes worden opgelezen of hardware waarmee de tekens voelbaar worden gemaakt. Op deze wijze kunnen vertrouwensdiensten door mensen met een visuele beperking worden gebruikt. Er zijn in Nederland geen praktijksituaties bekend waarbij een persoon met een handicap een vertrouwensdienst wilde gebruiken maar dit vanwege zijn beperking onmogelijk was. De verordening bepaalt dat waar dat haalbaar is, vertrouwensdiensten en eindgebruikersproducten, die worden gebruikt bij de verlening van deze diensten toegankelijk worden gemaakt voor personen met een handicap. Overweging 29 van de verordening geeft aan dat de haalbaarheidsbeoordeling niet alleen op technische, maar ook op economische overwegingen moet worden gebaseerd. De verordening bevat hiermee reeds een verplichting voor vertrouwensdienstverleners in hun aanbod rekening te houden met personen met een handicap indien er toegankelijkheidsproblemen optreden, voor zover dat althans technisch en economisch gezien haalbaar is.

De leden van de CDA-fractie vroegen zich af waarom de webrichtlijnen, waarmee de toegankelijkheid voor mensen met een handicap wordt geborgd, wel voor overheden verplicht zijn maar niet gelden voor niet-overheden. De verplichting voor overheden om te voldoen aan de webrichtlijnen vloeit voort uit een bestuursakkoord. Voor websites is er een internationaal breed geaccepteerde en toegepaste standaard voor web toegankelijkheid (ISO-, NEN- en EU-norm). Dit is de zogenaamde

internationale open standaard «web content accessibility guidelines» (WCAG) http://www.w3.org/Translations/WCAG20-nl/. Steeds meer Nederlandse websites gebruiken deze standaard om een toegankelijke website te hebben. Het kabinet acht het echter niet wenselijk deze verplicht te stellen voor niet-overheden, omdat deze eisen kunnen leiden tot een disproportionele toename van kosten en administratieve lasten. Onder Nederlands voorzitterschap wordt momenteel onderhandeld over een richtlijn van de Europese Unie die toegankelijkheid van overheids-websites verplicht stelt. Daarbij is de vraag in hoeverre deze standaard niet alleen voor overheden maar ook voor bepaalde bedrijven zou moeten gaan gelden.

De leden van de CDA-fractie vroegen in hoeverre bedrijven kunnen worden gestimuleerd om vertrouwensdiensten technisch toegankelijk te maken voor personen met een handicap. Zoals in antwoord op eerdere vragen van de leden van de SP-fractie in deze paragraaf is aangegeven, slagen de Nederlandse vertrouwensdienstverleners er in om hun vertrouwensdiensten voldoende toegankelijk te maken voor personen met een handicap. Het stimuleren hiertoe vanuit de overheid is dan ook niet nodig.

6. Rechtsgevolgen bij gebruik van vertrouwensdiensten

6.1 Bewijs en rechtsgevolgen

De leden van de PVV-fractie vragen zich af waarom Nederlandse burgers gebruik zouden willen maken van een niet-gekwalificeerde vertrouwens-dienst, en of de regering hiervoor niet zou moeten waarschuwen. Niet-gekwalificeerde vertrouwensdiensten kunnen goedkoper en gebruikersvriendelijker zijn dan gekwalificeerde vertrouwensdiensten. Dat maakt het aantrekkelijk om ze te gebruiken. Het hangt van de toepassing en daarmee samenhangende risicobeoordeling af waarvoor een niet-gekwalificeerde vertrouwensdienst wordt gebruikt om te bepalen of die daar ook geschikt voor is. Een tijdstempel voor verkeer waaraan geen fatale termijnen of andere grote (juridische) gevolgen verbonden zijn, zal niet perse de gekwalificeerde variant vereisen. Dan kan het naar het keuze van betrokkenen ook volstaan om gebruik te maken van een goedkopere en/of makkelijker bruikbare niet-gekwalificeerde vertrouwensdienst. Er is dan ook geen reden om te waarschuwen voor het gebruik van niet-gekwalificeerde vertrouwensdiensten. Niet-gekwalificeerde vertrou-wensdiensten kunnen technisch en functioneel onderling verschillen en daarmee ook de betrouwbaarheid daarvan. Het is van belang dat dit voldoende inzichtelijk is voor de gebruikers van deze diensten en wat passend is voor toepassingen. De Handreiking betrouwbaarheidsniveaus van het Forum Standaardisatie helpt hierbij.

6.2 Uitvoeringsmaatregelen

7. Erkenning van vertrouwensdiensten

7.1 Erkenning van elektronische handtekeningen en zegels

De leden van de D66-fractie vroegen of het nodig is om voor elektronische diensten anders dan de elektronische handtekening een nationale algemene regeling te treffen over rechtsgevolgen of het vermoeden van integriteit en juistheid. Voor deze elektronische diensten kent ons nationaal recht geen algemene regeling over rechtsgevolgen of over het vermoeden van integriteit en juistheid. De verordening zelf bepaalt dat voor andere vertrouwensdiensten dan de elektronische handtekening, te weten de elektronische zegels, tijdstempels en diensten voor elektro-

nische aangetekende bezorging, geldt dat de gekwalificeerde elektronische methode daarvan het vermoeden van integriteit en juistheid oplevert. Daar het vermoeden door de verordening zelf wordt geregeld, is voor een nationale regeling geen plaats. De verordening vereist voor deze diensten geen nadere uitwerking. Of andere vertrouwensdiensten tot een rechtsgevolg leiden of kunnen leiden is afhankelijk van nationaal recht (overweging 22). Anders dan bij de elektronische handtekening geldt voor geen van de andere vertrouwensdiensten dat er gelijkschakeling is met een fysieke variant. Een regeling zoals voor de elektronische handtekening ligt dan ook niet voor de hand.

De leden van de D66-fractie verzochten om toelichting bij ondertekening met een geavanceerde handtekening en cloudoplossingen. Een van de eisen voor een geavanceerde elektronische handtekening is dat de gegevens die de ondertekenaar gebruikt om te ondertekenen onder zijn controle zijn. Dit kan doordat de ondertekenaar de gegevens fysiek in zijn eigen bezit heeft. In dat geval vallen controle en beheer van de gegevens waarmee de handtekening wordt gezet samen. Door het gebruik van mobiele apparaten is er een behoefte om ook in die omgevingen te ondertekenen. Een methode waarmee dit zonder gebruik van hardware, zoals een smartcard en een paslezer, door de gebruiker eenvoudig mogelijk kan worden gemaakt is om controle en beheer van de aanmaakgegevens voor elektronische handtekeningen te scheiden. De ondertekenaar kan de gegevens dan onafhankelijk van de ICT-omgeving gebruiken om te ondertekenen. Op deze wijze houdt de ondertekenaar de uitsluitende controle over de gegevens terwijl het beheer van de gegevens door een derde partij, zoals een vertrouwensdienstverlener, wordt verricht. De verordening biedt hiervoor de ruimte, maar stelt als voorwaarde dat de ondertekenaar de aanmaakgegevens «met een hoog vertrouwensniveau» onder zijn uitsluitende controle kan gebruiken. In de handreiking Betrouwbaarheidsniveaus voor elektronische overheidsdiensten (versie 3) van het Forum Standaardisatie wordt op verschillende mogelijkheden nader ingegaan.

8. Gegevensbescherming

De leden van de VVD-fractie vroegen om nadere uitleg of een toenemend aantal knooppunten niet leidt tot een verzwakking van de beveiliging. Ieder knooppunt vormt een risico en vanuit het oogpunt van beveiliging betekent een toename van het aantal knooppunten een toename van de risico’s en een verzwakking van de beveiliging. Zoals in de beantwoording van een vraag van de leden van de D66-fractie in paragraaf 4.3 over het creëren van één gemeenschappelijk knooppunt is aangegeven, vormt één centraal knooppunt echter ook een veiligheidsrisico. Een gedecentraliseerde structuur waarbij ieder land één, of maximaal enkele knooppunten heeft, is het model waar de lidstaten uiteindelijk voor gekozen hebben.

De leden van de VVD-fractie vroegen zich af op welke termijn de aangekondigde aanvullende «Privacy Impact Assessments» worden uitgevoerd. In antwoord op een eerdere soortgelijke vraag van de leden van de PvdA-fractie in paragraaf 4.2 is aangegeven dat de aanvullende PIA in de zomer van 2016 word uitgevoerd en in het najaar beschikbaar wordt gesteld aan de Kamer.

De leden van de VVD-fractie informeerden of de aanvullende «Privacy Impact Assessments» vóór of na wijziging van de eidas-uitvoeringswet wordt uitgevoerd. De uitvoering van een aanvullende «Privacy Impact Assessment» is voorzien in de zomer van 2016. Dit is twee jaar voordat de erkenning van elektronische identificatiemiddelen verplicht wordt. Voor de verplichte erkenning van vertrouwensdiensten, die losstaat van het

knooppunt, geldt een ander tijdpad. Het onderdeel vertrouwensdiensten treedt namelijk op 1 juli 2016 in werking. De voorgestelde wijzigingen in het wetsvoorstel tot aanpassing van bestaande wetten richt zich uitsluitend op vertrouwensdiensten.

De leden van de SP-fractie informeerden naar de voorzorgsmaatregelen om de bescherming van persoonsgegevens te waarborgen in het geval gekozen gaat worden voor beheer door een private partij. Indien er gekozen wordt voor het onderbrengen van het eIDAS-knooppunt bij een private partij zal er sprake zijn van een bewerker in de zin van artikel 1, sub e, van de Wet bescherming persoonsgegevens. Daarbij is de Minister van Economische Zaken dan verantwoordelijke in de zin van artikel 1, sub d, van de Wet bescherming persoonsgegevens. Tussen de Minister en de bewerker wordt dan een bewerkersovereenkomst gesloten waarin ondermeer de beveiliging van het eIDAS-knooppunt wordt geregeld. Daarbij gelden dan dezelfde eisen als die nu gelden in de huidige situatie waarin het eIDAS-knooppunt in beheer van de Minister is.

De leden van de SP-fractie wilden weten op welke manier tot een eventuele keuze voor de bewerking van persoonsgegevens voor het eIDAS-knooppunt door marktpartijen zal worden gekomen en op welke wijze de Kamer daarbij betrokken wordt. De besluitvorming over het inschakelen van marktpartijen bij het beheer van het knooppunt zal pas over enige jaren plaatsvinden. Van een bewerker in de zin van de Wet bescherming persoonsgegevens zal alleen sprake zijn wanneer hier aantoonbare voordelen aan vast zitten. Hiervan kan bijvoorbeeld sprake zijn als een tweede knooppunt wenselijk wordt geacht vanuit het belang van continuïteit om storingen met het eerste knooppunt op te vangen. Wanneer het eIDAS-knooppunt door een marktpartij goedkoper kan worden beheerd dan binnen de overheid zelf, zonder dat hiervoor concessies aan de veiligheid of bescherming van persoonsgegevens worden gedaan, kan overwogen worden om een marktpartij als bewerker van de Minister te laten optreden. Deze afweging zal pas aan de orde zijn indien het gebruik van het eIDAS-knooppunt sterk toeneemt. Indien de Kamer dit wil wordt ze bij de besluitvorming hieromtrent betrokken.

De leden van de SP-fractie informeerden in hoeverre, als dit knooppunt wordt beheerd door een Idensys-partij, de Minister van Binnenlandse Zaken betrokken zal worden bij beperking en oplossing van ontstane problemen. De Minister van Economische Zaken is en blijft verantwoordelijk voor het huidige eIDAS-knooppunt. Wanneer het knooppunt door een Idensys-partij wordt beheerd is er sprake van bewerkerschap, waarbij die partij ten behoeve van en onder verantwoordelijkheid van de Minister van Economische Zaken persoonsgegevens verwerkt. In de bewerkersovereenkomst worden zaken zoals de beveiliging en beschikbaarheid van het knooppunt geregeld. Eventuele problemen zullen dan ook in de relatie tussen de Minister en de bewerker worden opgelost. De betrokkenheid van de Minister van Binnenlandse Zaken en Koninkrijksrelaties wordt bepaald door de eigen verantwoordelijkheid van deze miniser voor een nationaal stelsel, waarbij gebruik wordt gemaakt van het eIDAS-knooppunt. Door de Minister van Binnenlandse Zaken en Koninkrijkrelaties en de Minister van Economische Zaken zullen afspraken worden gemaakt over de beperking en de oplossing van van eventuele problemen met het eIDAS-knooppunt, waarbij recht wordt gedaan aan ieders verantwoordelijkheid.

De leden van de SP-fractie waren benieuwd of in het geval van bijvoorbeeld identiteitsdiefstal of het doorgeleiden van verkeerde gegevens protocollen zullen worden opgesteld om problemen zo snel mogelijk te beperken en op te lossen. Voor het doorgeven van verkeerde persoonsi-

dentificatiegegevens aan een andere lidstaat moet eerst in Nederland onderzocht worden wat daarvan de oorzaak is. Als het gaat om fouten of identiteitsdiefstal waarbij een enkele persoon wordt geraakt dan moet in de eerste plaats zijn elektronische identificatiemiddel worden ingetrokken. Wanneer de betrouwbaarheid van het stelsel als geheel in het geding is, bevat de verordening verplichtingen om hiermee om te gaan. Indien er op grote schaal identiteitsdiefstal heeft plaatsgevonden heeft de lidstaat de verplichting het aangemelde stelsel voor elektronische identificatie «onverwijld» op te schorten of in te trekken, en de andere lidstaten en de Commissie hierover te informeren. De elektronische identificatiemiddelen van die lidstaat kunnen dan niet langer in andere lidstaten worden gebruikt.

De leden van de CDA-fractie vroegen om een toelichting op welke wijze in dit wetsvoorstel de privacy wordt gewaarborgd bij de verwerking van persoonsgegevens. Het wetsvoorstel zelf bevat geen voorschriften ten aanzien van de verwerking van persoonsgegevens. De verordening en de uitvoeringshandelingen bevat wel bepalingen ten aanzien van de verwerking van persoonsgegevens bij het grensoverschrijdend gebruik van elektronische identificatiemiddelen. Bij grensoverschrijdend gebruik van elektronische identificatiemiddelen wordt slechts een minimale dataset doorgegeven. Het betreft de voornaam, achternaam, geboorteplaats en geboortedatum. Deze gegevens worden versleuteld via het knooppunt doorgegeven aan andere lidstaten. De knooppunten worden beveiligd en zullen de gegevens slechts doorgeven waarbij er sprake is van kortstondige technische opslag. Op het knooppunt zelf en de aansluiting daarvan op het nationale stelsel voor elektronische identificatie en authenticatie worden Privacy Impact Assessments uitgevoerd. Daarnaast wordt het knooppunt voortdurend gemonitord als onderdeel van het beheer. Dit zijn maatregelen die worden getroffen om te voldoen aan de Wet bescherming persoonsgegevens.

De leden van de CDA-fractie vroegen of de aangekondigde aanvullende «Privacy Impact Assessments» naar de Kamer kan worden gestuurd. Het antwoord hierop is bevestigend. De aanvullende Privacy Impact Assessment zal, wanneer deze gereed is, naar de Kamer worden gestuurd. De planning is om de PIA in de zomer uit te voeren waarna de rapportage in het najaar gereed zal zijn en naar de Kamer wordt gezonden.

8.1 Gegevensbescherming

De leden van de CDA-fractie vroegen zich af waarom elektronische identificatie geldt bij zowel natuurlijke personen als bij rechtspersonen. Vanwege het belang van een digitale interne markt is het wenselijk om de wederzijdse erkenning van zowel elektronische identificatiemiddelen van natuurlijke als van rechtspersonen te regelen. Zowel natuurlijke personen als rechtspersonen kunnen namelijk gebruik maken van elektronische identificatiemiddelen om transacties te doen met openbare instanties in andere lidstaten. Burgers kunnen bijvoorbeeld hun kinderen aanmelden op een school in een andere lidstaat of elektronisch inzage krijgen in hun opgebouwde pensioen als zij in een andere lidstaat hebben gewerkt. Rechtspersonen maken echter ook gebruik van elektronische diensten waarbij identificatie en authenticatie nodig is. Voorbeelden hiervan zijn intermediairs die namens rechtspersonen belastingaangifte doen, vergunningen aanvragen, jaarrekeningen deponeren etc.
De leden van de PVV-fractie refereerden aan het eIDAS-knooppunt en vroegen om een uitputtende lijst waar de elektronische identificatie uitruildienst voor benut wordt. Er is geen sprake van uitruilen maar van het doorgeven van persoonsidentificatiegegevens aan een openbare instantie waar een burger of bedrijf op elektronische wijze een dienst van

wil afnemen. Op dit moment kan geen uitputtend overzicht gegeven worden van alle onlinediensten aangeboden door openbare instanties in de 27 lidstaten waar een verplichting voor erkenning van elektronische identificatiemiddelen uit andere lidstaten voor zal gaan gelden. Op http://ec.europa.eu/internal_market/eu-go/index_en.htm staan echter de portalen voor bedrijven opgesomd. Naar verwachting zullen de portalen die op deze website genoemd staan, ontsloten moeten worden voor elektronische identificatiemiddelen voor bedrijven uit andere lidstaten. Voor burgers zijn de bijvoorbeeld volgende portalen bekend bij de Minister van Economische Zaken. Op deze portalen staan verwijzingen naar overheidsdiensten waarvoor een elektronische identiteit benodigd is:

1. https://www.eesti.ee/est/
2. https://www.overheid.nl/
3. https://www.service-public.fr/
4. https://www.gov.uk/
5. http://administracion.gob.es/
6. https://www.portaldocidadao.pt/en
7. http://www.lineaamica.gov.it/
8. http://www.gov.ie/
9. https://www.gov.hr/
10. https://www.help.gv.at
11. http://portal.gov.cz/
12. http://www.cyprus.gov.cy
13. http://www.ermis.gov.gr
14. https://www.latvija.lv/
15. https://www.borger.dk/
16. http://e-guvernare.ro/
17. https://obywatel.gov.pl/
18. http://www.guichet.public.lu/
19. https://www.slovensko.sk
20. http://evem.gov.si
21. https://mygov.mt/
22. http://www.suomi.fi
23. https://ugyfelkapu.magyarorszag.hu/
24. http://www.nap.bg/
25. https://www.skatteverket.se/
26. http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Anwendungen_node.html
27. https://www.island.is/en/public-services
28. http://www.norge.no/en
29. http://www.llv.li/#/20/

De overheidsdiensten die toegankelijk zijn met DigiD zijn te vinden op: https://www.digid.nl/over-digid/wie-doen-mee/. De overheidsdiensten die toegankelijk zijn met eHerkenning zijn hier te vinden: https://www.eherkenning.nl/aansluiten-op-eherkenning/wie-zijn-aangesloten/. Op de beide genoemde websites staan ook private partijen genoemd. Private partijen vallen buiten de plicht om identificatiemiddelen uit andere lidstaten te erkennen.

De leden van de PVV vroegen zich af of Nederlandse openbare instanties zonder dat een betreffende persoon daarvan op de hoogte is gegevens over de elektronische identiteit kan versturen naar andere EU-lidstaten. Het versturen van persoonsindentificatiegegevens tussen overheden wordt niet door de verordening of het wetsvoorstel geregeld. De uitwisseling van persoonsgegevens door Nederland met openbare instanties in andere lidstaten wordt geregeld door de Wet bescherming persoonsgegevens. De regels zijn dat er alleen gegevens mogen worden doorgegeven wanneer er sprake is van een wettelijke verplichting (artikel 8c, van de Wet bescherming persoonsgegevens) of wanneer dit noodza-

kelijk is voor de goede uitvoering van een publiekrechtelijke taak (artikel 8 e, van de Wet bescherming persoonsgegevens). Het eIDAS-knooppunt zal alleen gegevens doorsturen indien een burger zelf zich met een elektronisch identificatiemiddel in verbinding wil stellen met een openbare instantie in een ander EU-land. De elektronische verwerking van persoonsidentificatiegegevens vindt derhalve per definitie met toestemming van de betrokken persoon zelf plaats.

De leden van de PVV-fractie vroegen zich af, als de vorige vraag instemmend wordt beantwoord, waarvoor deze mogelijkheid benut wordt behoudens criminele zaken?
Zoals uit het vorige antwoord op de vragen van de PVV-fractie blijkt is er in het kader van de verordening geen sprake van het doorsturen van gegevens indien de burger daartoe zelf niet besluit. De gegevensuitwisseling met andere lidstaten van andere gegevens is geregeld door de Wet Bescherming Persoonsgegevens of door sectorale wetgeving.

De leden van de PVV-fractie vroegen zich af op welke wijze de Nederlandse burger gebaat is bij de uitwisseling van elektronische gegevens binnen EU-lidstaten zonder de persoonlijke toestemming van de betreffende burger. Door het gebruik van zijn elektronische identiteit geeft de burger toestemming voor het gebruik van de minimale dataset door de ontvangende openbare instantie. Deze gegevens zijn nodig voor het verlenen van toegang tot digitale dienstverlening die in het belang van de burger is. Wanneer de burger zijn elektronische identificatiemiddel niet wil gebruiken, zal hij op andere wijze met de openbare instantie moeten communiceren, bijvoorbeeld via formulieren. Er is derhalve geen sprake van uitwisseling van persoonsidentificatiegegevens met openbare instanties in andere lidstaten zonder dat de burger hier iets vanaf weet of waar de burger niets aan heeft.

De leden van de PVV-fractie vroegen zich af waarom een lidstaat bij een incident met elektronische identiteiten niet het betreffende bedrijf of de burger zou informeren, en vroegen zich voorts af welke andere reden dan omwille van de publieke opinie incidenten met het Europese elektronische identiteiten systeem aan hen niet kenbaar worden gemaakt. De Europese Commissie is niet bevoegd om te bepalen dat bedrijven of burgers moeten worden geïnformeerd over incidenten met lidstaten. Het is aan de lidstaten zelf om dit te bepalen. Wanneer dit in het belang is van burgers en bedrijven zullen deze worden geïnformeerd over incidenten met elektronische identiteiten, zodat er maatregelen genomen kunnen worden om de gevolgen van het incident te beperken. De publieke opinie speelt hierbij geen rol.

De leden van de PVV-fractie vroegen zich af in hoeverre de Kamer geïnformeerd wordt over vertrouwensbreuken in het elektronische identiteiten knooppunt. Bij het optreden van een vertrouwensinbreuk in het eIDAS-knooppunt zal de Minister van Economische Zaken de Tweede Kamer hierover informeren.

8.2 Uitvoeringsmaatregelen

De leden van de D66-fractie stelden vast dat het knooppunt de integriteit van gegevens moet waarborgen en verzochten om uitleg welke maatregelen voor de bescherming van persoonsgegevens en informatiebeveiliging getroffen worden. De te nemen maatregelen voor de bescherming van de persoonsgegevens in het knooppunt zijn uiteengezet in het antwoord op een eerdere vraag van de leden van de CDA-fractie over bescherming van privacy bij dit wetsvoorstel. Ten aanzien van de

informatiebeveiliging verwijs ik naar het antwoord op de vragen van de leden van de VVD-fractie over beheer van het knooppunt in paragraaf 2.1. De leden van de D66-fractie vernamen dat situaties zoals storingen en identiteitsdiefstal zoveel mogelijk door «adequate beveiliging» voorkomen moeten worden en vroegen om een definitie van «adequate beveiliging». Deze leden wilden bovendien weten welke stappen al zijn gezet om deze adequate beveiliging te realiseren, naast de verschillende maatregelen die al genoemd worden.
De ICT-beheerorganisatie van het Ministerie van Economische Zaken, die het knooppunt beheert en door ontwikkelt, voldoet aan de ISO 27001 norm. Dit is de gangbare norm die het begrip «adequaat beveiliging» concrete invulling geeft en toetsbaar maakt. Daarnaast wordt het gebruik van het knooppunt voortdurend gemonitord.

10. Administratieve lasten en verdere effecten voor het bedrijfsleven

De leden van de VVD-fractie verzochten of de regering bereid is de toekomstige lasten, die uit het wetsvoorstel en de verordening voortvloeien, in de gaten te houden en zo laag mogelijk te houden. Beperking van de administratieve lasten van de verordening is en blijft een belangrijk aandachtspunt. Concreet krijgt deze beperking vorm doordat het wetsvoorstel uitsluitend strekt tot uitvoering van de verordening en daarnaast door samenwerking tussen de toezichthouders en het NCSC bij de melding van inbreuken op de veiligheid en integriteit.

De leden van de CDA-fractie verzochten om cijfermatig aan te geven hoe groot de toename van de administratieve lasten is voor de aanbieders van vertrouwensdiensten en overheden van dit wetsvoorstel. Deze leden wilden weten waar de verwachte stijging van administratieve lasten voor gekwalificeerde aanbieders van vertrouwensdiensten uit bestaat. Tot slot vroegen deze leden zich af welke verplichtingen het wetsvoorstel te weeg brengt voor het midden- en kleinbedrijf.
De verordening en het wetsvoorstel leiden niet tot administratieve lasten voor overheden. De stijging van administratieve lasten voor de aanbieders van gekwalificeerde vertrouwensdiensten vloeit voort uit de verplichtingen van de verordening. Deze lasten hangen samen met het aantal soorten vertrouwensdiensten dat de dienstverlener aanbiedt en het aantal meldingen dat moet worden gedaan. Door de verbreding van het toepassingsbereik van de verordening ten opzichte van de Richtlijn elektronische handtekeningen komen vertrouwensdiensten onder toezicht die daar voorheen buiten vielen. Voordat gekwalificeerde vertrouwensdiensten als zodanig aan het publiek mogen worden aangeboden, moet de toezichthouder hebben vastgesteld of deze diensten aan de wettelijke eisen voldoen. De lasten die samenhangen met de aanvraag van de status gekwalificeerd hangen af van het aantal soorten gekwalificeerde diensten dat de dienstverlener wil aanbieden. Per aanvraag moet een aantal vragen van de toezichthouder worden beantwoord en een conformiteitbeoordelingsverslag worden overlegd. Het beantwoorden van de vragen van de toezichthouder zal maximaal twee uur in beslag nemen. Bij een uurtarief van 50 Euro zullen de lasten ongeveer 100 Euro per aanvraag bedragen. De kosten van een conformiteitbeoordeling zijn niet exact aan te geven. De ervaring met de gekwalificeerde elektronische handtekening leidt tot een inschatting van 40.000 Euro voor een conformiteitsbeoordelingsverslag. Daarbij geldt dat de werkzaamheden voor meerdere gekwalificeerde vertrouwensdiensten tegelijkertijd zullen worden verricht waardoor de toezichtslasten en kosten hiervan lager uit zullen vallen. Het doen van een melding voor een veiligheidsinbreuk of integriteitsverlies veroorzaakt eveneens administratieve lasten. Bij het melden van de nog vast te stellen basis set gegevens, moeten enkele vragen worden

beantwoord. Het beantwoorden van deze vragen zal maximaal twee uur in beslag nemen. Bij een uurtarief van 50 Euro komen de administratieve lasten uit op maximaal 100 Euro per melding. Per aanbieder worden niet meer dan enkele meldingen per jaar verwacht. Bij omvangrijke incidenten zullen de administratieve lasten hoger uitvallen vanwege de beantwoording van vervolgvragen van de betrokken toezichthouder(s) en het NCSC. Deze administratieve lasten vallen echter in het niet bij het verlies van de dienstverlening dat een bedrijf in een dergelijk geval kan hebben. Gezien de aard van de dienstverlening betekent het verlies van vertrouwen immers dat de basis onder de dienstverlening compleet zal wegvallen. Het wetsvoorstel en de verordening bevatten geen verplichtingen voor het midden- en kleinbedrijf.

10.1 Elektronische identiteiten

De leden van de D66-fractie constateerden dat de private sector niet verplicht is om zich aan te sluiten bij de verplichte erkenning van elektronische identiteiten uit andere lidstaten, maar dat dit wel mogelijk is en vroegen of nader ingegaan kan worden op de gevolgen voor de wetswijziging voor de private sector, waaronder de verschillen tussen de effecten voor de publieke sector en de private sector en welke het belangrijkste zijn. Het wetsvoorstel strekt uitsluitend tot uitvoering vande verordening en verplicht de private sector niet tot erkenning van elektronische identificatiemiddelen uit andere lidstaten. Het wetsvoorstel heeft dan ook geen gevolgen voor de private sector. Wanneer de private sector dit wil, en het gebruik van het eIDAS-knooppunt hiervoor wordt toegestaan, kan de private sector elektronische identificatiemiddelen uit andere landen erkennen. De verordening, en niet het wetsvoorstel, verplicht openbare instanties tot erkenning van elektronische identificatiemiddelen van het niveau «substantieel» of «hoog» uit andere lidstaten. De verordening heeft geen gevolgen voor de private partijen, tenzij deze ervoor kiezen om tot erkenning van elektronische identificatiemiddelen uit andere lidstaten over te gaan en het eIDAS-knooppunt hiervoor open wordt gesteld. De gevolgen van de verordening voor openbare instanties zijn dat deze in september 2018 in staat moeten zijn om te gaan met elektronische identificatiemiddelen uit andere lidstaten.

10.3 Toezichtlasten

De leden van de CDA-fractie verzochten of door middel van het wetsvoorstel de rol van de toezichthouder dient te worden uitgebreid en welke kosten dit met zich meebrengt.
De verordening en de voorgestelde uitvoering daarvan in Nederland zullen tot aanpassing en uitbreiding van de rol van de toezichthouder leiden. Zoals in het antwoord op een eerdere vraag van de leden van de CDA-fractie over administratieve lasten in paragraaf 10 is aangegeven, vloeit de voorgenomen uitbreiding voort uit de verbreding van het toepassingsbereik van de verordening waardoor meer vertrouwensdiensten dan voorheen onder toezicht zullen komen te vallen. Naast deze uitbreiding in de breedte vindt ook uitbreiding in de diepte plaats. De rol van de toezichthouder wordt aangepast, waarbij er onder meer sprake zal zijn van eigen onderzoek en oordeelsvorming van de toezichthouder dan voorheen. In antwoord op een eerdere vraag van de leden van de PvdA-fractie in paragraaf 5.8 over het schrappen van het vermoeden van overeenstemming is hier reeds op ingegaan. Voor het toezicht op de verordening wordt 7 fte ingezet. De kosten hiervan bedragen 1.325.042 Euro per jaar.
De leden van de PVV-fractie vroegen zich af wanneer er meer duidelijkheid over de stijging van toezichtlasten kan worden verschaft en of de regering bereid is de verdere behandeling van het wetsvoorstel op te schorten tot

dat er een compleet beeld is van de financiële impact van dit wetsvoorstel. Inmiddels is er meer inzicht in de administratieve lasten van de verordening, waaronder in het bijzonder ook de toezichtlasten. In antwoord op een eerdere vraag in paragraaf 10 van de leden van CDA-fractie over de stijging van administratie lasten is ingegaan op de stijging van de toezichtlasten. De voornaamste lasten die ook voor het toezicht van belang zijn, bestaan standaard uit de conformiteitsbeoordeling die op 40.000 Euro wordt geschat. De lasten dalen naarmate er meer gekwalificeerde vertrouwensdiensten worden meegenomen in de conformiteitsbeoordeling. De meerkosten bedragen dan naar verwachting maximaal enkele duizenden Euro's per vertrouwensdienst. De lasten van het beantwoorden van de vragen van de toezichthouder bij het aanvragen van de status gekwalificeerd bedragen eveneens ongeveer 100 Euro per vertrouwensdienst. De lasten per initiële melding zullen maximaal 100 Euro per bedrijf bedragen. Het is niet aan de orde om de behandeling van het wetsvoorstel op te schorten wegens gebrek aan inzicht in de administratieve lasten.

De leden van de D66-fractie wilden weten welke private partijen en overheidsorganisaties gekwalificeerde vertrouwensdiensten leveren en gebruiken. De leden vragen wanneer bekend wordt in hoeverre deze partijen gekwalificeerde diensten gaan aanbieden. Gekwalificeerde certificaten voor elektronische handtekeningen worden momenteel geleverd door KPN B.V., ESG De Electronische signatuur B.V., Digidentity B.V. en QuoVadis, het Ministerie van Defensie, het Ministerie van Infrastructuur en Milieu en het CIBG, een uitvoeringsorganisatie van het Ministerie van Volksgezondheid Welzijn en Sport. Uit een inventarisatie van Agentschap Telecom blijkt dat alle aanbieders verder gaan met de uitgifte van gekwalificeerde certificaten voor elektronische handtekeningen en dat enkele organisaties plannen hebben om gekwalificeerde certificaten voor de authenticatie van websites, gekwalificeerde certificaten voor elektronische zegels en gekwalificeerde elektronische tijdstempels aan te bieden. Partijen bepalen zelf wanneer ze een aanvraag voor de status gekwalificeerd voor een vertrouwensdienst bij een toezichthouder indienen. Voor wat betreft de private partijen is dit interne bedrijfsinformatie die niet bij de overheid bekend is. Van de overheidsorganisaties is de verwachting dat deze hun huidige vertrouwensdiensten onder de verordening zullen continueren.

11. Financiële gevolgen voor medeoverheden

13. Internetconsultatie

De leden van de CDA-fractie wilden weten welke extra kosten het Ministerie van Economische Zaken in 2018 voor medeoverheden via het Gemeente- en Provinciefonds zal compenseren, conform de verplichtingen uit de Financiële Verhoudingswet. Naar de kosten van de implementatie van de verordening is onderzoek verricht (onderzoek Financiële gevolgen Europese verordening elektronische identiteiten en vertrouwensdiensten voor medeoverheden, Ecorys, 2013). Uit dit onderzoek blijkt dat de kosten van de verordening voor wat betreft erkenning van elektronische identiteiten voornamelijk bestaan uit aansluiting op het eIDAS-knooppunt en aanpassing van de website. Deze kosten zullen, conform de verplichtingen van de Financiële Verhoudingswet, via het Gemeente- en Provinciefonds worden gecompenseerd. Het gaat om circa 1.000 Euro per organisatie aan eenmalige kosten.

De leden van de CDA-fractie verzochten om een bevestiging dat er geen bezuiniging zal plaatsvinden op de compensatie via het Gemeente- en Provinciefonds. In aanvulling op de vorige vraag van deze leden merk ik

op dat alleen de werkelijke kosten, die met de implementatie van de verordening, zijn gemoeid worden gecompenseerd. Er bestaat geen voornemen om hierop te bezuinigen, zodat de Minister van Economische Zaken als verantwoordelijke voor het eIDAS-knooppunt het verzoek kan bevestigen.

Deze leden van de CDA-fractie vroegen naar de voorwaarden voor deelname door de Waterschappen aan het Europese financieringsprogramma, de «Connecting Europe Facility» en in hoeverre dit haalbaar is. De «Connecting Europe Facility», afgekort tot CEF, bestaat uit financiële middelen die de Europese Commissie beschikbaar stelt om onder meer de verbintenis van digitale infrastructuren tussen de lidstaten te bevorderen. Nederland doet mee met dit programma en in het kader hiervan kunnen de Waterschappen, met gebruik van de financiële middelen van de Commissie, aansluiten op het knooppunt. De voorwaarde is dat Waterschappen diensten elektronisch toegankelijk moeten maken voor natuurlijke en/of niet natuurlijke personen door aansluiting op het knooppunt. Wanneer de Waterschappen hiervoor capaciteit beschikbaar stellen, is het haalbaar om aan het project mee te doen en zodoende aan te sluiten op het knooppunt.

De leden van de CDA-fractie vroegen of de regering kan aangeven in hoeverre is overwogen om bepaalde spanningsvelden tussen security en privacy op andere manieren op te lossen in plaats van met wetgeving. De verordening heeft tot doel grensoverschrijdende erkenning van elektronische identificatiemiddelen en vertrouwensdiensten mogelijk te maken. Het doel van de verordening is daarmee niet primair gericht op het oplossen van spanningsvelden tussen veiligheid en privacy. Voor wat betreft erkenning van elektronische identificatiemiddelen uit andere lidstaten is er ter uitvoering van de verordening op nationaal niveau uitsluitend sprake van feitelijke uitvoering van de verordening, waarbij uitgangspunten terzake van dataminimalisatie en «privacy bij design» in acht zullen worden genomen. Hier is de reeds bestaande Wet bescherming persoonsgegevens op van toepassing. Voor wat betreft vertrouwensdiensten strekt het wetsvoorstel niet verder dan ter uitvoering van de verordening. Het delen van best practices, scholing, het leren van inbreuken en het opstellen en gebruiken van standaarden zijn voorbeelden van alternatieven voor wetgeving om met bescherming van persoonsgegevens en beveiligingsvraagstukken om te gaan.

De leden van de PvdA-fractie vroegen waarom de toepassing van artikel 12 van de Wet raadgevend referendum alsnog is geschrapt na het advies van de Raad van State. Het wetsvoorstel regelde dat bij het inwerkingtredingsbesluit zo nodig toepassing wordt gegeven aan artikel 12 van de Wet raadgevend referendum bij de inwerkingtreding van artikelen of onderdelen van het voorstel van wet die zijn gewijzigd na indiening van het voorstel bij de Tweede Kamer. Hiermee werd beoogd te anticiperen op de eventuele situatie dat in de parlementaire behandeling onderwerpen aan het wetsvoorstel worden toegevoegd die de verplichte uitvoering van de verordening te buiten gaan. De Afdeling merkt op dat het uitgangspunt bij implementatie van bindende EU regelgeving is dat in de implementatieregeling geen andere regels worden opgenomen dan voor de implementatie noodzakelijk zijn. De Afdeling wijst er onder meer op dat het opnemen van een bepaling waarin artikel 12 van de Wet raadgevend referendum wel van toepassing wordt, geen recht doet aan het uitgangspunt van die wet dat artikel 12 uitsluitend in uitzonderingsituaties moet worden toegepast. De reden voor toepassing van artikel 12 zal, blijkens de toelichting op de Wet raadgevend referendum, geen andere kunnen zijn dan dat de wet dermate spoedeisend is dat afgeweken moet worden van de algemene inwerkingtredingsprocedure uit de artikelen 8

en 9 van de Wet raadgevend referendum. Deze spoedeisendheid dient in zo'n geval dan ook gemotiveerd te worden. Het voor de zekerheid opnemen van een bepaling die artikel 12 van de Wet raadgevend referendum van toepassing verklaart, voor het geval toepassing ervan in de loop van de parlementaire behandeling wenselijk blijkt, voldoet niet aan dit uitgangspunt. Gelet op de door de Afdeling gegeven overwegingen is naar aanleiding daarvan het bewuste artikel over de toepassing van artikel 12 geschrapt.

De leden van de PvdA-fractie verzochten aan te geven welke volkenrechtelijke organisatie wordt bedoeld en of de Europese Commissie als zodanig is op te vatten. Artikel 5, aanhef en onderdeel e, van de Wet raadgevend referendum bepaalt dat geen referendum kan worden gehouden over wetten die uitsluitend strekken tot uitvoering van verdragen of besluiten van volkenrechtelijke organisaties. De verordening is een besluit van de Europese Unie, die een volkenrechtelijke organisatie is in de zin van het aangehaalde artikelonderdeel. De Europese Commissie is een onderdeel van de Europese Unie en daarmee niet zelf een volkenrechtelijke organisatie.

De leden van de PvdA-fractie vroegen zich verder af of er dan niet heel veel wetten niet onder Wet raadgevend referendum vallen en hoe zich dit dan tot het referendum over het Associatieverdrag met Oekraïne verhoudt. Tot besluiten van volkenrechtelijke organisaties zijn onder meer verordeningen en richtlijnen van de Europese Unie te rekenen. Alle wetten die ter implementatie en uitvoering hiervan strekken, zijn derhalve op grond van artikel 5, aanhef en onderdeel e, van de Wet raadgevend referendum niet referendabel. De zingeving daarvan is dat de lidstaten bij de uitvoering van dergelijke besluiten geen beleidsvrijheid toekomt ten aanzien de doeleinden daarvan en een raadgevend referendum dus niet zinvol wordt geacht. Het raadgevend referendum van 6 april jl. had betrekking op een wet houdende goedkeuring van de associatieovereenkomst met Oekraïne en viel dus buiten de reikwijdte van artikel 5, aanhef en onderdeel e, van de Wet raadgevend referendum. De goedkeuring van verdragen zoals dat met Oekraïne, is uitdrukkelijk wel onder de werking van de Wet raadgevend referendum gebracht.

De leden van de PvdA-fractie vroegen zich af waarom waterschappen niet gecompenseerd worden voor extra kosten en waarom zij naar de «Connecting Europe Facility» worden verwezen. De Waterschappen worden niet genoemd in artikel 2 van de Financiële Verhoudingswet. Daarom hebben de waterschappen geen recht op compensatie op grond van deze wet. Als de Waterschappen meedoen met het Nederlandse project van de Connecting Europe Facility kunnen ze met gebruik van Europees geld aansluiten op het knooppunt.

De leden van de PvdA-fractie vroegen of de provincies en gemeenten tevreden zijn over de aan hen aangeboden compensatie. Op dit moment zijn er geen signalen dat gemeenten en provincies ontevreden zijn over de berekende compensatie. Zoals in antwoord op een eerdere soortgelijke vraag van de leden van de CDA-fractie in deze paragraaf is aangegeven, zullen alleen de werkelijke kosten voor het voldoen aan de verplichtingen van de verordening worden gecompenseerd. Deze kosten zijn in 2013 onderzocht. Wanneer in de praktijk blijkt dat de kosten van implementatie hoger uitvallen, waardoor gemeenten en provincies reden zouden kunnen hebben tot ontevredenheid, zullen de kosten opnieuw worden onderzocht en wordt de compensatie daarop aangepast. Overigens zal de compensatie in 2018 worden uitgekeerd wanneer de verplichte erkenning van elektronische identiteiten in werking treedt.

De leden van de PvdA-fractie vroegen of de decentrale overheden Idensys inmiddels goed in beeld hebben. De beantwoording van deze vraag staat los van het wetsvoorstel. De decentrale overheden zijn allen bekend met DigiD en de meesten ook met eHerkenning. Aan de bekendheid van de ontwikkeling naar Idensys wordt aandacht besteed. Deze ontwikkelingen zijn nog betrekkelijk nieuw waardoor niet alle decentrale overheden ze even scherp op het netvlies zullen hebben.

De leden van de PvdA-fractie vroegen hoe dit wetsvoorstel zich verhoudt tot de bredere Digitale Interne Markt. De leden vroegen wanneer de volgende wetsvoorstellen hierover worden ingediend. Het wetsvoorstel strekt tot implementatie van de verordening. De verordening is onderdeel van de Digitale Agenda voor Europa uit 2010. Op 6 mei 2015 heeft de Europese Commissie haar strategie voor de Europese digitale interne markt gepubliceerd. Het realiseren van een digitale interne markt is een van de tien politieke prioriteiten van de Commissie-Juncker. De hierin aangekondigde Europese voorstellen voor regelgeving betreffen het e-commerce pakket. Dit bevat wetgeving op het gebied van geo-blocking, pakketbezorging en herziening van een verordening betreffende samenwerking met betrekking tot consumentenbescherming.

De leden van de D66-fractie informeerden of de regering kan ophelderen dat Nederland geen afgifte van een gekwalificeerd certificaat met een elektronisch identificatiemiddel van het niveau «hoog» kan toestaan, terwijl tegelijkertijd wordt gesteld dat een openbare instantie geen elektronisch identificatiemiddel hoeft te erkennen dat een lager betrouwbaarheidsniveau heeft dan voor de online dienst vereist is. Deze leden vroegen zich ook af of dit niet tegenstrijdig is. Voorafgaand aan de afgifte van een gekwalificeerd certificaat moet de identiteit zijn geverifieerd van de degene aan wie een gekwalificeerd certificaat wordt afgegeven (artikel 24, eerste lid, eerste alinea, van de verordening). De verordening definieert de mogelijkheden hiervoor. Een van die mogelijkheden is dat de identiteit voorafgaand aan de afgifte van een gekwalificeerd certificaat op afstand wordt geverifieerd door middel van een elektronisch identificatiemiddel waaraan in hoofdstuk II van de verordening het niveau «substantieel» of «hoog» wordt toegekend. Gekwalificeerde vertrouwensdienstverleners hebben het recht deze wijze van identiteitsverificatie te gebruiken. Nederland kan er dan ook niet voor kiezen om alleen een afgifte van een gekwalificeerd certificaat met een elektronisch identificatiemiddel van niveau «hoog» toe te staan. Wel geldt dat de vertrouwensdienstverlener dit elektronische identificatiemiddel alleen mag accepteren voor identiteitsverificatie bij afgifte van een certificaat indien is gewaarborgd dat de afgifte daarvan in de fysieke aanwezigheid van de natuurlijke persoon of gemachtigde afgevaardigde van de rechtspersoon heeft plaatsgevonden (artikel 24, eerste lid, onderdeel b, van de verordening). Deze wijze van identiteitsverificatie voor gekwalificeerde certificaten leidt niet tot tegenstrijdigheid. Anders dan voor de op Europees niveau in de verordening geregelde gekwalificeerde certificaten en verleners daarvan, betreft het bij de erkenning van aangemelde stelsels van elektronische identificatiemiddelen nationaal ingerichte of nationaal geregelde stelsels die een onderling verschillend betrouwbaarheidsniveau kunnen hebben. De verordening voorziet er daarom in dat die nationale bij de Europese Commissie aangemelde stelsels worden ingedeeld in het op een nationaal stelsel van toepassing zijnde betrouwbaarheidsniveau «laag», «substantieel of «hoog». Een openbare instantie hoeft vervolgens niet een elektronisch identificatiemiddel te erkennen dat een lager betrouwbaarheidsniveau heeft dan voor de onlinedienst vereist is. De wijze van identiteitsverificatie bij gekwalificeerde certificaten als hiervoor bedoeld, is daarvan te onderscheiden.

De leden van de D66-fractie vroegen of het voor Nederland mogelijk is alleen elektronische identificatiemiddelen te erkennen van het niveau «hoog», en zo nee waarom niet. Openbare instanties of lidstaten kunnen zelf het betrouwbaarheidsniveau bepalen van elektronische identificatiemiddelen waarmee toegang tot hun onlinediensten kan worden verkregen. Welke betrouwbaarheidsniveaus vervolgens grensoverschrijdend erkend moeten worden, is daarvan afhankelijk. Openbare instanties in Nederland die voor toegang tot hun eigen online dienstverlening een elektronisch identificatiemiddel eisen of voorschrijven met het betrouwbaarheidsniveau «hoog», hoeven uitsluitend bij de Europese Commissie aangemelde elektronische identificatiemiddelen uit andere lidstaten te erkennen die eveneens over het betrouwbaarheidsniveau «hoog» beschikken. Een openbare instantie hoeft in dat geval dus niet elektronische identificatiemiddelen uit een andere lidstaat te erkennen met een lager betrouwbaarheidsniveau dan «hoog». De vaststelling van een betrouwbaarheidsniveau is in de praktijk afhankelijk van de toegankelijkheid en beschikbaarheid voor burgers en ondernemers van elektronische identificatiemiddelen met een beoogd betrouwbaarheidsniveau. Tevens hangt het van de aard en inhoud van een specifieke onlinedienst of samenstel van onlinediensten af welk betrouwbaarheidsniveau (minimaal) volstaat.

De leden van de D66-fractie vroegen zich af, welke stappen de regering neemt om ervoor te zorgen dat Nederland slechts elektronische identificatiemiddelen erkent van het niveau «hoog». Nederland kan de erkenning van elektronische identiteiten niet beperken tot niveau hoog. De aanbieders van publieke diensten in Nederland bepalen zelf het vereiste betrouwbaarheidsniveau voor toegang tot hun diensten. Vereist een dienstaanbieder een middel met betrouwbaarheidsniveau «hoog», dan moeten Nederlandse en buitenlandse gebruikers inloggen met een middel met dit betrouwbaarheidsniveau. Op dit moment zijn middelen met een hoog betrouwbaarheidsniveau in Nederland nog niet breed uitgerold. Wanneer de dienstverlener betrouwbaarheidsniveau substantieel vraagt aan Nederlandse natuurlijke en niet-natuurlijke personen dan verplicht de verordening tot erkenning van middelen uit andere lidstaten die dit betrouwbaarheidsniveau hebben.

II. ARTIKELEN

Artikel V (artikel 2:16 Awb)

Aan de leden van de CDA-fractie kan worden bevestigd dat geavanceerde en andere elektronische handtekeningen hetzelfde rechtsgevolg kunnen hebben als een handgeschreven of een gekwalificeerde elektronische handtekening als de methode voor ondertekening die gebruikt is voldoende betrouwbaar is gelet op de aard en inhoud van het elektronische bericht en doel waarvoor het is gebruikt. Op de vraag hoe die betrouwbaarheid wordt vastgesteld, is hiervoor uitgebreid ingegaan bij de beantwoording van de vragen van de leden van de PvdA-fractie over artikel 2:16 Awb (zie paragraaf 4.1 van deze nota).

De Minister van Economische Zaken,
H.G.J. Kamp